ON THE DENSITY OF GENERATING PAIRS IN FINITE PROJECTIVE SPECIAL LINEAR GROUPS AND PROJECTIVE SYMPLECTIC GROUPS OF ODD CHARACTERISTIC

By

ÁRON BERECZKY

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

1998

Copyright 1998

by

ÁRON BERECZKY

ACKNOWLEDGEMENTS

I thank the members of my Supervisory Committee, Dr. Thompson, Dr. Turull, Dr. Bodine, Dr. Keesling and Dr. Voelklein for their friendly support and encouragement throughout the four years of my studies at the University of Florida.

I consider it a great privilege to have worked with Professor John G. Thompson as one of his students and I am most grateful to him for giving me this opportunity.

I would also like to thank Professor Robert Guralnick of the University of Southern California for suggesting me the research field of the spread of finite simple groups, it turned out to be an exciting topic for my dissertation.

I am especially grateful to Professor Alexandre Turull for his helpful comments and suggestions, and for the numerous conversations we have had about my research and about finite classical groups.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii

ABSTRACT v

CHAPTERS

1 INTRODUCTION 1

2 SINGER ELEMENTS AND THEIR MAXIMAL OVERGROUPS . . 7

- 2.1 Singer Cycles 7
- 2.2 Extension Field Type Subgroups 19
- 2.3 Maximal Overgroups of Singer Elements 30

3 CENTRALIZER ORDERS 46

- 3.1 Elements of Order p with Homogeneous Action in GL Groups . . 46
- 3.2 Elements of Order p with Homogeneous Action in Sp Groups . . 47
- 3.3 Elements of Order p with Homogeneous Action in GU Groups . . 68
- 3.4 Arbitrary Elements of Order p in GL, Sp and GU Groups 82
- 3.5 Centralizer Orders of p'-Elements in GL, Sp and GU Groups . . 91

4 FIXED POINT RATIOS ON THE COSETS OF EXTENSION FIELD TYPE SUBGROUPS 103

- 4.1 Notations and Some Technical Lemmas 103
- 4.2 Case I: p'-Elements Centralizing an Extension Field 105
- 4.3 Case II: p'-Elements Acting Non-Trivially on an Extension Field 132
- 4.4 Case III: Elements of Order p Centralizing an Extension Field . . 158
- 4.5 Case IV: Elements of Order p Acting Non-Trivially on an Extension Field 170
- 4.6 Upper Bounds for the Fixed Point Ratios of Arbitrary Elements 176

5 LOWER BOUNDS FOR THE CARDINALITY OF A(G) 178

REFERENCES 189

BIOGRAPHICAL SKETCH 190

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

ON THE DENSITY OF GENERATING PAIRS IN FINITE PROJECTIVE SPECIAL LINEAR GROUPS AND PROJECTIVE SYMPLECTIC GROUPS OF ODD CHARACTERISTIC

By

ÁRON BERECZKY

December 1998

Chairman: Dr. John G. Thompson
Major Department: Mathematics

This research investigates the spread of two families of finite simple groups, the projective special linear groups and the projective symplectic groups in odd characteristic. A group G has spread k if for any given set $\mathcal{S}$ of nontrivial elements with cardinality k in G, there exists an element g in G such that $\langle g, s\rangle = G$ for any $s \in \mathcal{S}$. Another approach is the following. A set $\mathcal{S}$ of nontrivial elements in G is called an anti-generating set if for any $g \in G$ there is an $s \in \mathcal{S}$ such that $\langle g, s\rangle$ is a proper subgroup of G. If we denote the smallest cardinality of an anti-generating set in G by $A(G)$ then the group G has spread $A(G) - 1$. The goal of this paper is to find non-trivial lower bounds for $A(G)$ in the case when G is a finite projective special linear group or a finite projective symplectic group in odd characteristic. As some partial results, we classify the maximal subgroups containing Singer cycles in the special linear groups and in the symplectic groups of odd characteristic, we provide

some formulas for the orders of centralizer subgroups of p'-elements and elements of order p, where p is the characteristic, and calculate some upper bounds for the fixed point ratios in the primitive permutation representations on the cosets of extension field type maximal subgroups.

CHAPTER 1
INTRODUCTION

Since the completion of the classification of finite simple groups it is well-known that every finite simple group can be generated by two of its elements. However, the history of studying the generator pairs in finite simple groups reaches back to the 19th century. It was conjectured first by E. Netto in [12] that if two elements are randomly chosen from the alternating group A_n, they will generate A_n with probability $\to 1$ as $n \to \infty$. This conjecture was proved by J. D. Dixon in [3], who also conjectured that a similar result holds for arbitrary finite simple groups. Namely, if $P(G)$ denotes the probability that two randomly chosen elements of a finite simple group G generate G, then $P(G) \to 1$ as $|G| \to \infty$. The proof of Dixon's conjecture was completed by W. Kantor, A. Lubotzky, M. Liebeck and A. Shalev [7, 8]. Their work relies on the classification of finite simple groups, in particular on the information about the maximal subgroups of finite simple groups, obtained from the classification.

Another famous problem about the generating pairs of finite simple groups, that has been studied throughout this century is the so-called (2,3)-generating problem. A group G is (2,3)-generated if it has a pair of generators $\{x, y\}$ satisfying $x^2 = y^3 = 1$. The motivation behind the study of the existence of such generating pairs is the fact that a group G is (2,3)-generated if and only if it is a homomorphic image of the classical modular group $\mathrm{PSL}_2(\mathbf{Z})$. Although not every finite simple group is (2,3)-generated, most of them have been proved to be so. For more details and recent results, see for example, Liebeck and Shalev [9] and Lubeck and Malle [10]. It is also a fact that except $\mathrm{PSU}_3(9)$, every finite simple group is generated by an involution and a strongly real element. In particular, every finite simple group is generated by three involutions, except $\mathrm{PSU}_3(9)$, which is known to be generated by four involutions.

Let us call a set $\mathcal{S}$ of nontrivial elements in a finite simple group G an *anti-generating* set if for any g in G there is an s in $\mathcal{S}$ that the pair $\{s, g\}$ generates only a proper subgroup in G. Furthermore, let $A(G)$ be the smallest possible cardinality of an anti-generating set in G. It was proven by R. Guralnick and W. Kantor [4] that $A(G) \geq 2$ for any finite simple group G. In other words, any nontrivial element of a finite simple group belongs to a pair of generators. As of today, it is still an open question whether $A(G) \geq 3$ for all finite simple groups G. Asymptoticly, $A(G) \to \infty$ as $|G| \to \infty$ if we omit the alternating and odd-dimensional orthogonal groups. This was proven by Guralnick and Kantor [4].

In this paper, I will give lower bounds for $A(G)$ when G is a finite projective special linear group or a finite projective symplectic group in odd characteristic. The results are summarized in the following theorems:

Main Theorem 1 *Let $G = PSL_d(q)$ with $d \geq 3$ and $(d, q) \neq (3, 4)$.*

(a) If d is a prime number and $q = 2$ then

$$A(G) \geq \frac{2^{(d-1)^2}}{7(d-1)} \; ;$$

(b) If d is a prime number and $q = 3$ then

$$A(G) \geq \frac{3^{(d-1)^2}}{3(d-1)} \; ;$$

(c) If d is a prime number and $q \geq 4$ then

$$A(G) \geq \frac{q^{(d-1)^2}}{2(d-1)} \; ;$$

(d) If $d = 4$ and $q = 2$ then $A(G) \geq 6$;

(e) If $d = 4$ and $q = 3$ then $A(G) \geq 20$;

(f) If $d = 4$ *and* $q \geq 4$ *then* $A(G) \geq \frac{1}{3} \cdot q^4$;

(g) If $d = 6$ *then* $A(G) \geq q^d - 2$;

(h) If $d > 6$ *and* d *is not a prime then* $A(G) \geq q^d$.

Actually, if r *is the smallest prime divisor of* d *and* $r \geq 3$ *then* $A(G) \geq q^{(r-1)d} - q^{(r-3)d} + 1$.

Main Theorem 2 *Let* $G = PSp_d(q)$ *with* q *odd and* $(d,q) \neq (4,3)$, $(2,3)$, $(2,5)$, $(2,7)$ *or* $(2,9)$.

(a) If $d = 2$ *and* $q \equiv 1 \pmod 4$ *then* $A(G) \geq q$;

(b) If $d = 2$ *and* $q \equiv 3 \pmod 4$ *then* $A(G) \geq \frac{q(q-1)}{q+3}$;

(c) If $d = 4$ *then* $A(G) \geq q$;

(d) If $d = 6$ *then* $A(G) \geq q^4 - 3q^2$;

(e) If $d = 2r$ *with a prime number* $r \geq 5$ *then* $A(G) \geq q^{d-2}$;

(f) If $d = 2r$ *with* r *an odd composite number then* $A(G) \geq q^{d-2} - q^{d-4}$;

(g) If $d \equiv 0 \pmod 4$ *and* $d \geq 8$ *then* $A(G) \geq q^{\frac{1}{2}d}$.

Main Theorem 3 *Let* $G \simeq PSL_2(q)$ *with* $q \geq 4$.

(a) If q *is even then* $A(G) = q - 1$;

(b) If $q \equiv 1 \pmod 4$ *and* $q \geq 13$ *then* $A(G) = q$;

(c) If $q \equiv 3 \pmod 4$ *and* $q \geq 11$ *then* $A(G) \geq q - 3$;

(d) If $q = 5$ *or* $q = 9$ *then* $A(G) = 3$;

(e) If $q = 7$ *then* $A(G) = 5$.

The approach I use is based on an idea introduced by Guralnick and Kantor [4] and it is the following:

Let G be a finite group, $\mathcal{C}$ be a conjugacy class of G and

$$P_{\mathcal{C}} = \min_{1 \neq g \in G} \Pr\{c \in \mathcal{C} \mid \langle c, g \rangle = G\} .$$

That is, for any fixed nontrivial element g in G, the probability that a randomly chosen element in $\mathcal{C}$ will generate G together with g is at least $P_{\mathcal{C}}$. Of course, if $\mathcal{S}$ is an anti-generating set in G then

$$1 \le \sum_{s\in\mathcal{S}} \Pr\{c \in \mathcal{C} \mid \langle c, s\rangle \neq G\} \le \sum_{s\in\mathcal{S}} (1 - P_{\mathcal{C}}) = |\mathcal{S}| \cdot (1 - P_{\mathcal{C}}) ,$$

and therefore

$$A(G) \ge \frac{1}{1 - P_{\mathcal{C}}} .$$

Because of this, it seems to be reasonable to look for the best conjugacy class in this sense in every finite simple group G, that is, to find the conjugacy class $\mathcal{C}$ of G with the highest possible $P_{\mathcal{C}}$, and then of course, calculate the actual value of $P_{\mathcal{C}}$, or at least find a useful lower bound for it. In order to calculate a lower bound for $P_{\mathcal{C}}$ for a particular conjugacy class $\mathcal{C}$, it turns out to be helpful if one has a complete list of the maximal subgroups of G that have a non-trivial intersection with $\mathcal{C}$. The reason for this is quite simple. Suppose c is a fixed element of $\mathcal{C}$ and let $\mathcal{M}(c)$ denote the set of maximal overgroups of c in G. Furthermore, for any $M \in \mathcal{M}(c)$, and $g \in G$, let $N(G, M, g)$ denote the number of conjugates of M in G that contain g. Then for any $g \in G$,

$$\begin{aligned}
\Pr\{c' \in \mathcal{C} \mid \langle c', g\rangle \neq G\} &= \Pr\{a \in G \mid \langle c^a, g\rangle \neq G\} \\
&= \Pr\{a \in G \mid \exists M \in \mathcal{M}(c) \text{ such that } g \in M^a\} \\
&\le \sum_{M\in\mathcal{M}(c)} \Pr\{a \in G \mid g \in M^a\} \\
&= \sum_{M\in\mathcal{M}(c)} \frac{N(G, M, g)}{|G : M|} .
\end{aligned}$$

Actually, $\frac{N(G,M,g)}{|G:M|}$ is the ratio of fixed points of g in the primitive permutation representation of G on the cosets of M. So if we denote the maximal possible fixed point ratio of a nontrivial element on the cosets of M by $\mu(M)$ then we have

$$\begin{aligned} \Pr\{c' \in \mathcal{C} \mid \langle c', g\rangle \neq G\} &\leq \sum_{M \in \mathcal{M}(c)} \mu(M)\,, \\ 1 - P_{\mathcal{C}} &\leq \sum_{M \in \mathcal{M}(c)} \mu(M)\,, \end{aligned}$$

and

$$A(G) \geq \frac{1}{\sum_{M \in \mathcal{M}(c)} \mu(M)}\,.$$

This is the inequality I will use to obtain lower bounds for $A(G)$ when G is a finite projective special linear or a finite projective symplectic group.

My choice for the conjugacy class $\mathcal{C}$ is the class of so-called Singer elements. In $\mathrm{GL}_d(q)$, a cyclic subgroup is called a Singer cycle if it has order $q^d - 1$. In $\mathrm{SL}_d(q)$ or in $\mathrm{Sp}_d(q)$, a cyclic subgroup is called a Singer cycle if it is the intersection of a Singer cycle of $\mathrm{GL}_d(q)$ with $\mathrm{SL}_d(q)$ or $\mathrm{Sp}_d(q)$, and has order $(q^d-1)/(q-1)$ or $q^{\frac{d}{2}}+1$, respectively. In $\mathrm{PSL}_d(q)$ or $\mathrm{PSp}_d(q)$ a cyclic subgroup is called a Singer cycle if it is the image of a Singer cycle of $\mathrm{SL}_d(q)$ or $\mathrm{Sp}_d(q)$, respectively. And a Singer element in general is an element that generates a Singer cycle. Since the maximal overgroups of a Singer cycle in $\mathrm{PSL}_d(q)$ are in one-to-one correspondence with the maximal overgroups of its pre-image in $\mathrm{SL}_d(q)$, it is enough to calculate $\sum_{M \in \mathcal{M}(c)} \mu^*(M)$ for singer elements c in $\mathrm{SL}_d(q)$, where $\mu^*(M)$ denotes the maximal possible fixed point ratio of a non-central element on the cosets of M. A similar argument goes also for the PSp case. W. Kantor [6] proved that in $\mathrm{GL}_d(q)$, every maximal overgroup of a Singer cycle is an extension field type subgroup corresponding to a prime divisor r of d, that is, a subgroup isomorphic to $Z_r \ltimes \mathrm{GL}_{\frac{d}{r}}(q^r)$. In Chapter 2, after a general review on the Singer cycles and on the extension field type subgroups, we will prove a similar result for the Singer cycles in $\mathrm{SL}_d(q)$, and in $\mathrm{Sp}_d(q)$ for odd q. More precisely, except for $\mathrm{SL}_3(4)$, $\mathrm{Sp}_4(3)$ and $\mathrm{SL}_2(q) = \mathrm{Sp}_2(q)$ for $q = 3, 5, 7, 9$, the only maximal overgroups of Singer cycles are the intersections of the extension field type subgroups of $\mathrm{GL}_d(q)$ with $\mathrm{SL}_d(q)$ and $\mathrm{Sp}_d(q)$, respectively. The proof will be based on the results of a recent paper by R. Guralnick, T. Penttila, C. E. Praeger and J. Saxl [5]. This paper contains a classification of all the subgroups of $\mathrm{GL}_d(q)$ with order divisible by a primitive prime divisor of $q^d - 1$. (A prime r is called a primitive prime divisor of $q^d - 1$ if it divides $q^d - 1$ but does not divide $q^e - 1$ for any $1 \leq e < d$. It was proven first by K. Zsigmondy [14] that these primitive prime divisors always exist except when $(d, q) = (6, 2)$ or $d = 2$ and $q + 1$ is power of 2.)

The actual calculations for the upper bounds for the fixed point ratios are in Chapter 4, and they use the following formulas:

$$\mu(G, M, g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G, M, g)|}{|G|} = \frac{|M|}{|G|} \cdot \sum_{i=1}^{k} \frac{|C_G(g_i)|}{|C_M(g_i)|}$$

where $\mu(G, M, g)$ denotes the fixed point ratio of g on the cosets of M, $\mathcal{C}(G, M, g)$ is the set of elements in M that are conjugate to g in G and $\{g_1, \ldots, g_k\}$ is a set of representatives of the conjugacy classes in M that fall into the conjugacy class of g in G. In Case I we calculate upper bounds for the fixed point ratios of those elements having a prime order different from the characteristic and centralizing an extension field isomorphic to $\mathbf{F}_{q^r}$ for some prime divisor r of the dimension d, but not having any nontrivial action on other extension fields of $\mathbf{F}_q$ that are isomorphic to $\mathbf{F}_{q^r}$, involved in $\mathrm{GL}_d(q)$. In Case II we study those elements having a prime order, different from the characteristic and acting non-trivially on an extension field. In Case III and in Case IV we repeat the first two cases for elements of order p, where p is the characteristic. It is sufficient to calculate the upper bounds of the fixed point ratios only for these types of elements, because every non-central element in $\mathrm{GL}_d(q)$ with a positive fixed point ratio has a power that belongs to one of these categories. Notice that the two formulas mentioned above are heavily using the centralizer orders of elements with prime orders in the general linear and in the symplectic groups. Therefore, Chapter 3 is devoted to finding some explicit formulas of the centralizer orders needed in Chapter 4. The final results are proven in Chapter 5.

CHAPTER 2
SINGER ELEMENTS AND THEIR MAXIMAL OVERGROUPS

2.1 Singer Cycles

Definition 2.1.1 *A* **Singer element** *in a general linear group $GL_d(q)$ is an element whose order is $q^d - 1$.*

A Singer element in a special linear group $SL_d(q)$ is an element whose order is $\frac{q^d-1}{q-1} = q^{d-1} + q^{d-2} + \ldots + q + 1$.

A Singer element in a symplectic group $Sp_{2d}(q)$ is an element whose order is $q^d + 1$.

A Singer element in a general unitary group $GU_d(q^2)$ is an element whose order is $q^d - 1$.

A **Singer cycle** *in any of the above groups is a cyclic subgroup generated by a Singer element.*

Note, that Singer elements could be defined in SU, O, SO and in Ω groups also but we will not need them in this chapter.

Lemma 2.1.2 *There are Singer elements in every general linear, special linear or symplectic group, and in every unitary group of odd dimension.*

Proof: Take $V = \mathbf{F}_{q^d}$ as a vector space of dimension d over $\mathbf{F}_q$, and for any $a \in \mathbf{F}_{q^d}$ let $\hat{a}$ denote the multiplication by a on $\mathbf{F}_{q^d}$ as an $\mathbf{F}_q$-linear transformation. Then $\hat{a}$ is non-singular if and only if $a \neq 0$ and

$$S = \{\hat{a} \mid a \in \mathbf{F}^*_{q^d}\}$$

is a cyclic group of order $q^d - 1$ generated by any $\hat{a}$ such that $\langle a \rangle = \mathbf{F}^*_{q^d}$. This shows that S is a Singer cycle in $\mathrm{GL}(V) \simeq \mathrm{GL}_d(q)$.

The determinant of any $\hat{a}$ as an $\mathbf{F}_q$-linear transformation of V is actually the norm of a over $\mathbf{F}_q$, and since the norm map is an onto group homomorphism from $\mathbf{F}_{q^d}^*$ to $\mathbf{F}_q^*$,

$$S_1 = \{\hat{a} \mid a \in \mathbf{F}_{q^d}^*,\, \mathrm{N}(a) = 1\}$$

is a subgroup of S of order $\frac{q^d-1}{q-1}$ that is also a subgroup of $\mathrm{SL}(V) \simeq \mathrm{SL}_d(q)$.

Now suppose $d = 2e$, let Tr be the trace map from $\mathbf{F}_{q^d}$ to $\mathbf{F}_q$ and fix an element μ in $\mathbf{F}_{q^d}$ such that $\mu^{q^e-1}+1 = 0$. Such a μ always exists since $(-1)^{\frac{q^d-1}{q^e-1}} = (-1)^{q^e+1} = 1$ and it implies that -1 is a $(q^e-1)^{\text{th}}$ power in $\mathbf{F}_{q^d}$. Consider the form

$$\begin{aligned} B_1 : \mathbf{F}_{q^d} \times \mathbf{F}_{q^d} = V \times V \quad &\longrightarrow \quad \mathbf{F}_q \\ (a,b) \quad &\longmapsto \quad \mathrm{Tr}(\mu a b^{q^e}) . \end{aligned}$$

Then for any $a, b, c \in V$ and $\alpha \in \mathbf{F}_q$

$$\begin{aligned} B_1(\alpha a, b) &= \mathrm{Tr}(\alpha\mu a b^{q^e}) = \alpha\,\mathrm{Tr}(\mu a b^{q^e}) = \alpha\, B_1(a,b)\,, \\ B_1(a+b, c) &= \mathrm{Tr}(\mu(a+b)c^{q^e}) = \mathrm{Tr}(\mu a c^{q^e}) + \mathrm{Tr}(\mu b c^{q^e}) \\ &= B_1(a,c) + B_1(b,c)\,, \\ B_1(b,a) &= \mathrm{Tr}(\mu b a^{q^e}) = \mathrm{Tr}\big((\mu b a^{q^e})^{q^e}\big) = \mathrm{Tr}(\mu^{q^e} b^{q^e} a) \\ &= \mathrm{Tr}(-\mu a b^{q^e}) = -\mathrm{Tr}(\mu a b^{q^e}) = -B_1(a,b)\,. \end{aligned}$$

This shows that B_1 is a symplectic $\mathbf{F}_q$-bilinear form on V. The non-singularity of B_1 comes from the fact that the map Tr is a non-trivial additive group homomorphism from $\mathbf{F}_{q^d}$ to $\mathbf{F}_q$. Let $I(V, B_1)$ denote the isometry group of (V, B_1), so $I(V, B_1) \simeq \mathrm{Sp}_{2e}(q)$ and $S \cap I(V, B_1)$ is a cyclic group of order $q^e + 1$:

$$\begin{aligned} \hat{\alpha} \in I(V, B_1) \quad &\Longleftrightarrow \quad B_1(a\alpha, b\alpha) = B_1(a,b) \quad \forall\, a, b \in V \\ &\Longleftrightarrow \quad \mathrm{Tr}(\mu a b^{q^e} \alpha^{q^e+1}) = \mathrm{Tr}(\mu a b^{q^e}) \quad \forall\, a, b \in V \\ &\Longleftrightarrow \quad \mathrm{Tr}(x\alpha^{q^e+1}) = \mathrm{Tr}(x) \quad \forall\, x \in V \\ &\Longleftrightarrow \quad \mathrm{Tr}(x(\alpha^{q^e+1} - 1)) = 0 \quad \forall\, x \in V \\ &\Longleftrightarrow \quad \alpha^{q^e+1} = 1\,. \end{aligned}$$

Hence there is a Singer cycle in $\mathrm{Sp}_d(q)$.

Next, suppose that d is odd and $q = q_1^2$. Let Tr be the trace map as above, from $\mathbf{F}_{q^d}$ to $\mathbf{F}_q$, and consider the form

$$\begin{aligned} B_2 : \mathbf{F}_{q^d} \times \mathbf{F}_{q^d} = V \times V &\longrightarrow \mathbf{F}_q \\ (a, b) &\longmapsto \mathrm{Tr}(ab^{q_1^d}) \,. \end{aligned}$$

Then for any $a, b, c \in \mathbf{F}_{q^d} = V$ and $\alpha \in \mathbf{F}_q$

$$\begin{aligned} B_2(\alpha a, b) &= \mathrm{Tr}(\alpha a b^{q_1^d}) = \alpha \mathrm{Tr}(ab^{q_1^d}) = \alpha\, B_2(a,b)\,, \\ B_2(a+b, c) &= \mathrm{Tr}((a+b)c^{q_1^d}) = \mathrm{Tr}(ac^{q_1^d}) + \mathrm{Tr}(bc^{q_1^d}) \\ &= B_2(a,c) + B_2(b,c)\,, \\ B_2(b,a) &= \mathrm{Tr}(ba^{q_1^d}) = \mathrm{Tr}\big((ba^{q_1^d})^{q_1^{d+1}}\big) = \mathrm{Tr}(b^{q_1^{d+1}} a^{q_1}) \\ &= \big(\mathrm{Tr}(b^{q_1^d} a)\big)^{q_1} = B_2(a,b)^{q_1}\,. \end{aligned}$$

Here we used the assumption that d is odd, and thus everything in $\mathbf{F}_{q^d}$ is $\mathbf{F}_q$-conjugate to its q_1^{d+1}th power. The above equalities show that B_2 is a unitary form on $V = \mathbf{F}_{q^d}$. Again, the non-singularity of B_2 comes from the fact that the trace map from $\mathbf{F}_{q^d}$ to $\mathbf{F}_q$ is non-trivial. Let $I(V, B_2)$ denote the isometry group of (V, B_2), so $I(V, B_2) \simeq \mathrm{GU}_d(q) = \mathrm{GU}_d(q_1^2)$ and $S \cap I(V, B_2)$ is a cyclic group of order $q_1^d + 1$:

$$\begin{aligned} \hat{\alpha} \in I(V, B_2) &\iff B_2(a\alpha, b\alpha) = B_2(a,b) \quad \forall\, a, b \in V \\ &\iff \mathrm{Tr}(ab^{q_1^d} \alpha^{q_1^d+1}) = \mathrm{Tr}(ab^{q_1^d}) \quad \forall\, a, b \in V \\ &\iff \mathrm{Tr}(a\alpha^{q_1^d+1}) = \mathrm{Tr}(a) \quad \forall\, a \in V \\ &\iff \mathrm{Tr}(a(\alpha^{q_1^d+1} - 1)) = 0 \quad \forall\, a \in V \\ &\iff \alpha^{q_1^d+1} = 1\,. \end{aligned}$$

Hence there is a Singer cycle in $\mathrm{GU}_d(q) = \mathrm{GU}_d(q_1^2)$. ∎

Notice that there are no Singer elements in general unitary groups of even dimension. For if d is an even integer, then $q^{2d} - 1$ always has a primitive prime divisor r, which then divides q^d+1 but does not divide $|\mathrm{GU}_d(q^2)| = q^{\frac{d(d-1)}{2}}(q+1)(q^2-1)\dots(q^d-1)$. This makes it impossible for $\mathrm{GU}_d(q^2)$ to contain an element of order q^d+1.

Lemma 2.1.3 *A Singer cycle in a general linear, special linear, symplectic or general unitary group is always an irreducible linear group.*

Proof: Let $G = \mathrm{GL}_d(q)$, $\mathrm{SL}_d(q)$ or $\mathrm{Sp}_d(q)$ acting on a vector space V of dimension d over $\mathbf{F}_q$ and we may assume that $d \geq 2$. Let S be a Singer cycle in G, so

$$|S| = \begin{cases} q^d-1, & \text{if } G = \mathrm{GL}_d(q); \\ \frac{q^d-1}{q-1}, & \text{if } G = \mathrm{SL}_d(q); \\ q^{\frac{d}{2}}+1, & \text{if } G = \mathrm{Sp}_d(q). \end{cases}$$

Because of Maschke's Theorem, the action of S on V is semisimple, so either S is irreducible on V or $S \leq \mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$ for some proper subspaces V_1, V_2 of V with $V = V_1 \oplus V_2$.

If q^d-1 has a primitive prime divisor r, then r divides the order of S but does not divide the order of $\mathrm{GL}_e(q)$ for any $1 \leq e < d$, so S cannot be embedded into a direct product $\mathrm{GL}_e(q) \times \mathrm{GL}_{d-e}(q)$ with $1 \leq e < d$ and therefore S must have an irreducible action on V.

If q^d-1 does not have a primitive prime divisor then either $(d,q) = (6,2)$ or $d = 2$ and $q+1$ is a power of 2. Suppose $(d,q) = (6,2)$. Then

$$|S| = \begin{cases} 63, & \text{if } G \simeq \mathrm{GL}_6(2) = \mathrm{SL}_6(2); \\ 9, & \text{if } G \simeq \mathrm{Sp}_6(2). \end{cases}$$

Since $|\mathrm{GL}_5(2)| = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$ and the Sylow 3-subgroup of $\mathrm{GL}_5(2)$ is elementary abelian ($\mathbf{Z}_3 \times \mathbf{Z}_3$), there is no cyclic subgroup of order 9 in $\mathrm{GL}_e(2) \times \mathrm{GL}_{6-e}(2)$ for any $1 \leq e \leq 5$, and this implies that the action of S on V must be irreducible. Suppose $d = 2$ and $q+1 = 2^m$. Then clearly S must be an irreducible subgroup of $\mathrm{GL}(V)$, otherwise $S \simeq \mathbf{Z}_{2^m}$ would be isomorphic to a subgroup of $\mathrm{GL}_1(q) \times \mathrm{GL}_1(q) \simeq \mathbf{Z}_{2^m-2} \times \mathbf{Z}_{2^m-2}$, which is impossible.

Now let $G = \mathrm{GU}_d(q^2)$ acting on a vector space V of dimension d over $\mathbf{F}_{q^2}$, and let S be a Singer cycle in G. Then

$$|S| = q^d + 1 .$$

As in the other three cases, S has a semisimple action on V because of Maschke's Theorem and if $q^{2d} - 1$ has a primitive prime divisor r, then it forces S to act irreducibly on V. If $q^{2d} - 1$ does not have a primitive prime divisor then either $(d, q) = (3, 2)$ or $d = 1$ and $q + 1$ is a power of 2. In the $d = 1$ case there is nothing to prove, so assume that $(d, q) = (3, 2)$, in which case $G = \mathrm{GU}_3(4)$ and $|S| = 9$. The only way for S to have a proper invariant subspace in V is to be isomorphic to a subgroup of $\mathrm{GL}_2(4) \times \mathrm{GL}_1(4)$, but this is impossible since $|\mathrm{GL}_2(4) \times \mathrm{GL}_1(4)| = 2^6 \cdot 3^3 \cdot 5$ and its Sylow 3-subgroup is elementary abelian ($\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$). Therefore, S acts irreducibly on V. ∎

Lemma 2.1.4 *If A is a cyclic group and V is an irreducible $\mathbf{F}_q A$-module that has dimension d over $\mathbf{F}_q$ then*

$$End_{\mathbf{F}_q A}(V) \simeq \mathbf{F}_{q^d} .$$

Proof: First of all $\mathrm{End}_{\mathbf{F}_q A}(V)$ is a field because of Schur's Lemma. And this field contains $\mathbf{F}_q$ since all the scalar multiplications on V belong to $C_{\mathrm{GL}(V)}(A)$. So $\mathrm{End}_{\mathbf{F}_q A}(V) \simeq \mathbf{F}_{q^e}$ for some positive integer e and all we need to show is that $e = d$. Let $A = \langle a \rangle$ and let $p(x) \in \mathbf{F}_q[x]$ be the minimal polynomial of the action of a on V. Since V is irreducible under the action of A, $p(x)$ must be an irreducible polynomial over $\mathbf{F}_q$ and therefore the roots of $p(x)$ in an algebraic closure $\overline{\mathbf{F}_q}$ of $\mathbf{F}_q$ are all different. This implies that the matrix of a is diagonalizable over $\overline{\mathbf{F}_q}$ with all different entries in the main diagonal, so

$$\mathrm{End}_{\mathbf{F}_q A \otimes \overline{\mathbf{F}_q}}(V \otimes \overline{\mathbf{F}_q}) \simeq (\overline{\mathbf{F}_q})^d ,$$

$$\dim_{\mathbf{F}_q} \mathrm{End}_{\mathbf{F}_q A}(V) = \dim_{\overline{\mathbf{F}_q}} \mathrm{End}_{\mathbf{F}_q A \otimes \overline{\mathbf{F}_q}}(V \otimes \overline{\mathbf{F}_q}) = d ,$$

that is, $\dim_{\mathbf{F}_q} \mathbf{F}_{q^e} = d$ which clearly implies $e = d$. ∎

Lemma 2.1.5 *Let V be a vector space of dimension d over $\mathbf{F}_q$, v be a fixed nonzero vector in V and let S be a Singer cycle in $GL(V)$. Then for any vector w in V there is a unique element $e \in End_{\mathbf{F}_q S}(V)$ such that $ve = w$.*

Proof: By Lemmas 2.1.3 and 2.1.4 S acts irreducibly on V and $\mathrm{End}_{\mathbf{F}_q S}(V) \simeq \mathbf{F}_{q^d}$. So $|\mathrm{End}_{\mathbf{F}_q S}(V)| = |V| = q^d$ and it is enough to show that $e_1, e_2 \in \mathrm{End}_{\mathbf{F}_q S}(V)$, $e_1 \neq e_2$ implies $ve_1 \neq ve_2$. Since $\mathrm{End}_{\mathbf{F}_q S}(V)$ is a field, $e_1 \neq e_2$ implies that $(e_1 - e_2)e_3 = 1$ with some $e_3 \in \mathrm{End}_{\mathbf{F}_q S}(V)$, and then $v(e_1 - e_2)e_3 = v$, forcing $v(e_1 - e_2)$ to be a nonzero vector. Which means that $ve_1 \neq ve_2$. ■

Lemma 2.1.6 *A Singer cycle in a general linear group $GL_d(q)$ is always self centralizing and has index d in its normalizer.*

Proof: Let S be a Singer cycle in $\mathrm{GL}_d(q)$ acting on a vector space V of dimension d over $\mathbf{F}_q$ and let $E = \mathrm{End}_{\mathbf{F}_q S}(V)$. Then by Lemma 2.1.4 $E \simeq \mathbf{F}_{q^d}$ and so $|E| = q^d$. But on the other hand $|S \cup \{o\}| = q^d$ also and $S \subseteq C_{\mathrm{GL}(V)}(S) \subseteq E$, so $E = S \cup \{o\}$ and this means that S is its own centralizer in $\mathrm{GL}(V)$.

Let F be the field of scalar multiplications on V (which we may identify with the set of scalar matrices in $\mathrm{GL}_d(q)$ together with the zero matrix). Then $E|F$ is a Galois extension of degree d and for any $g \in N_{\mathrm{GL}(V)}(S)$ the conjugation by g on E is an automorphism of the field extension $E|F$. This way we get a natural homomorphism Ψ from $N_{\mathrm{GL}(V)}(S)$ to $\mathrm{Gal}(E|F)$ with $\ker(\Psi) = C_{\mathrm{GL}(V)}(S) = S$. This implies that $|N_{\mathrm{GL}(V)}(S) : S| \leq |\mathrm{Gal}(E|F)| = d$ and to prove the equality in here, we need to show that Ψ is an onto map.

Fix a nonzero vector v in V and for any $\sigma \in \mathrm{Gal}(E|F)$ define a linear transformation $\hat{\sigma}$ on V as follows.

$$\begin{aligned} \hat{\sigma} : V &\longrightarrow V \\ ve &\longmapsto ve^{\sigma} \qquad (\forall\, v \in V,\ e \in E)\,. \end{aligned}$$

This is well-defined by Lemma 2.1.5 and it is indeed a linear transformation as for any $e, f \in E$ and $\lambda \in F$

$$(ve + vf)\hat{\sigma} = v(e+f)\hat{\sigma} = v(e+f)^{\sigma} = ve^{\sigma} + vf^{\sigma} = ve\hat{\sigma} + vf\hat{\sigma} \;,$$

$$(\lambda ve)\hat{\sigma} = v(\lambda e)\hat{\sigma} = v(\lambda e)^{\sigma} = v\lambda e^{\sigma} = \lambda(v\hat{\sigma}) \;.$$

Furthermore, for any $e, f \in E$

$$(ve)(\hat{\sigma}^{-1} f \hat{\sigma}) = (ve^{\sigma^{-1}})f\hat{\sigma} = v(e^{\sigma^{-1}}f)^{\sigma} = (ve)f^{\sigma}$$

and thus $\hat{\sigma}^{-1} f \hat{\sigma} = f^{\sigma}$ showing that $\hat{\sigma} \in N_{\mathrm{GL}(V)}(S)$ and $\Psi(\hat{\sigma}) = \sigma$. So Ψ is indeed an onto map from $N_{\mathrm{GL}(V)}(S)$ to $\mathrm{Gal}(E|F)$ and as a result of this, $|N_{\mathrm{GL}(V)}(S) : S| = d$. ■

Lemma 2.1.7 *A Singer cycle in a symplectic group $Sp_d(q)$ or in a general unitary group $GU_d(q)$ is always self centralizing and has index d in its normalizer.*

Proof: Suppose B is a non-singular symplectic or unitary form on V, $I(V,B)$ is the isometry group of (V,B) and $S_1 = \langle s_1 \rangle$ is a Singer cycle in $I(V,B)$. Let $E = \mathrm{End}_{\mathbf{F}_q S_1}(V)$ and $S = E \setminus \{0\}$, then by Lemma 2.1.4 E is a field of cardinality q^d and hence S is a Singer cycle in $\mathrm{GL}(V)$. As in the previous lemma, let F be the subfield of E consisting of the scalar multiplications on V. Furthermore, let τ be the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_q}(V)$ such that

$$B(v\varphi, w) = B(v, w\tau(\varphi)) \quad \text{and} \quad B(v, w\varphi) = B(v\tau(\varphi), w)$$

for all $v, w \in V$ and $\varphi \in \mathrm{End}_{\mathbf{F}_q}(V)$. Since $s_1 \in I(V,B)$, $\tau(s_1) = s_1^{-1}$ and therefore τ stabilizes S_1 and also stabilizes $E = \mathrm{End}_{\mathbf{F}_q S_1}(V)$. In fact, τ acts on E as a field automorphism of E because it acts as a group automorphism on $S = E \setminus \{0\}$ for S is a cyclic group.

Now if the action of τ is the identity on E then $s_1 = \tau(s_1) = s_1^{-1}$ and $|s_1| = q^{\frac{d}{2}} + 1 \leq 2$ which is not possible, so τ must act on E as the involutionary field automorphism. That is, $\tau(e) = e^{q^{\frac{d}{2}}}$ for all $e \in E$. Then

$$\begin{aligned} x \in C_{I(V,B)}(S_1) &\iff x \in \mathrm{End}_{\mathbf{F}_q S_1}(V) \setminus \{0\} = E \setminus \{0\} \text{ and } \tau(x) = x^{-1} \\ &\iff x \in S \text{ and } x^{q^{\frac{d}{2}}} = x^{-1} \\ &\iff x \in S \text{ and } x^{q^{\frac{d}{2}}+1} = 1 \\ &\iff x \in S_1 \,. \end{aligned}$$

This proves that a Singer cycle in a symplectic or in a general unitary group is its own centralizer.

Next we want to show that $|N_{I(V,B)}(S_1) : S_1| = d$. Let $\Psi : N_{\mathrm{GL}(V)}(S) \to \mathrm{Gal}(E|F)$ as in the previous lemma and let Ψ_1 be the restriction of Ψ to $N_{I(V,B)}(S_1)$. (Notice that $N_{\mathrm{GL}(V)}(S) = N_{\mathrm{GL}(V)}(S_1)$ because S_1 is a characteristic subgroup in S and $S = C_{\mathrm{GL}(V)}(S_1)$, so $N_{I(V,B)}(S_1)$ is indeed a subgroup of $N_{\mathrm{GL}(V)}(S)$.)

Since $\ker(\Psi_1) = C_{I(V,B)}(S_1) = S_1$, the index of S_1 in $N_{I(V,B)}(S_1)$ cannot be larger than $|\mathrm{Gal}(E|F)| = d$ and in order to show that it is actually equal to d it is sufficient to show that Ψ_1 is an onto map.

For any $\sigma \in \mathrm{Gal}(E|F)$ define $\hat{\sigma} \in \mathrm{GL}(V)$ as in the previous lemma. That is, we fix a nonzero vector v in V and $(ve)\hat{\sigma} = ve^{\sigma}$ for all $e \in E$. As we saw it before, $\hat{\sigma}^{-1} f \hat{\sigma} = f^{\sigma}$ for any $f \in E$. This implies that

$$\tau(\hat{\sigma}) f \tau(\hat{\sigma})^{-1} = \tau(\hat{\sigma}^{-1} \tau(f) \hat{\sigma}) = \tau(\tau(f)^{\sigma}) = f^{\sigma}$$

for any $f \in E$, and hence $\hat{\sigma}\tau(\hat{\sigma})$ centralizes E, which can only happen if $\hat{\sigma}\tau(\hat{\sigma}) \in S$. Say $\hat{\sigma}\tau(\hat{\sigma}) = s^k$ where s is a generator element in S. Then

$$(s^k)^{q^{\frac{d}{2}}} = \tau(s^k) = \tau(\hat{\sigma}\tau(\hat{\sigma})) = \hat{\sigma}\tau(\hat{\sigma}) = s^k \,,$$

$$s^{k(q^{\frac{d}{2}}-1)} = 1$$

and so $q^{\frac{d}{2}+1}$ divides k. This implies that

$$\hat{\sigma}\tau(\hat{\sigma}) = s^k = z^{q^{\frac{d}{2}}+1} = z\tau(z)$$

for some $z \in S$. Now

$$(z^{-1}\hat{\sigma})\tau(z^{-1}\hat{\sigma}) = z^{-1}[\hat{\sigma}\tau(\hat{\sigma})]\tau(z)^{-1} = z^{-1}[z\tau(z)]\tau(z)^{-1} = 1 ,$$

which means that $z^{-1}\hat{\sigma} \in I(V, B)$. Also, $\Psi_1(z^{-1}\hat{\sigma}) = \Psi_1(\hat{\sigma}) = \sigma$. This shows that Ψ_1 is an onto map from $N_{I(V,B)}(S_1)$ to $\mathrm{Gal}(E|F)$ and therefore $|N_{I(V,B)}(S_1) : S_1| = d$. ■

Lemma 2.1.8 *The number of Singer cycles in $GL_d(q)$ is*

$$\frac{1}{d}q^{d(d-1)}\prod_{k=1}^{d-1}(1-\frac{1}{q^k})$$

and they are all conjugate to each other.

Proof: Let V be a vector space of dimension d over $\mathbf{F}_q$ and let S_1 and S_2 be two Singer cycles in $\mathrm{GL}(V)$. Let F denote the field of scalar multiplications on V and let $E_1 = \mathrm{End}_{\mathbf{F}_q S_1}(V)$, $E_2 = \mathrm{End}_{\mathbf{F}_q S_2}(V)$. Then E_1 and E_2 both contain F and by Lemma 2.1.4, $E_1 \simeq E_2 \simeq \mathbf{F}_{q^d}$. So there is a field isomorphism $\alpha : E_1 \to E_2$ that fixes F elementwise. Define a map g on V as follows. Let v be a fixed nonzero vector in V and let

$$\begin{aligned} g : V &\longrightarrow V \\ ve &\longmapsto ve^{\alpha} \quad (\forall\, e \in E_1) . \end{aligned}$$

This is a well-defined map by Lemma 2.1.5 and g is actually a nonsingular linear transformation on V as for any $e, f \in E$ and $\lambda \in F$

$$(ve + vf)g = v(e+f)g = v(e+f)^{\alpha} = v(e^{\alpha} + f^{\alpha}) = ve^{\alpha} + vf^{\alpha} = (ve)g + (vf)g ,$$

$$(\lambda ve)g = v(\lambda e)^{\alpha} = v\lambda e^{\alpha} = \lambda((ve)g) ,$$

$$vg = 0 \Longleftrightarrow ve^{\alpha} = 0 \Longleftrightarrow e^{\alpha} = 0 \Longleftrightarrow e = 0 \Longleftrightarrow ve = 0\,.$$

Furthermore, for any $e, f \in E_1$

$$(ve)(g^{-1}fg) = (ve^{\alpha^{-1}})fg = v(e^{\alpha^{-1}}f)^{\alpha} = vef^{\alpha}$$

and thus $g^{-1}fg = f^{\alpha}$ for any $f \in E_1$, showing that $g^{-1}E_1g = E_2$. Then it follows that

$$g^{-1}S_1g = g^{-1}(E_1 \setminus \{0\})g = E_2 \setminus \{0\} = S_2$$

so S_1 and S_2 are conjugate in $\mathrm{GL}(V)$, and this is true for any two Singer cycles in $\mathrm{GL}(V)$. Since by Lemma 2.1.2 the set of Singer cycles in $\mathrm{GL}(V)$ is non-empty and by Lemma 2.1.6 the order of the normalizer of a Singer cycle is $d(q^d-1)$, the number of Singer cycles in $\mathrm{GL}(V)$ must be $\frac{|\mathrm{GL}(V)|}{d(q^d-1)} = \frac{1}{d}q^{d(d-1)}\prod_{k=1}^{d-1}\left(1-\frac{1}{q^k}\right)$. ∎

Lemma 2.1.9 *The number of Singer cycles in $SL_d(q)$ is*

$$\frac{1}{d}q^{d(d-1)}\prod_{k=1}^{d-1}\left(1-\frac{1}{q^k}\right).$$

Proof: For every Singer cycle S in $\mathrm{GL}_d(q)$, $S_1 = S \cap \mathrm{SL}_d(q)$ is a subgroup of S with index $q-1$ and so S_1 is a Singer cycle in $\mathrm{SL}_d(q)$. On the other hand if S_1 is a Singer cycle in $\mathrm{SL}_d(q)$ acting on a vector space V of dimension d over $\mathbf{F}_q$ then by Lemma 2.1.3 S_1 acts irreducibly on V and by Lemma 2.1.4 $\mathrm{End}_{\mathbf{F}_qS_1}(V) \simeq \mathbf{F}_{q^d}$. So $S = \mathrm{End}_{\mathbf{F}_qS_1}(V) \setminus \{0\}$ is a Singer cycle in $\mathrm{GL}(V)$ with $S \cap \mathrm{SL}(V) = S_1$. This shows that there is a bijection between the set of Singer cycles in $\mathrm{GL}_d(q)$ and the set of Singer cycles in $\mathrm{SL}_d(q)$. Therefore, these two sets have the same cardinality, which is $\frac{1}{d}q^{d(d-1)}\prod_{k=1}^{d-1}\left(1-\frac{1}{q^k}\right)$ by Lemma 2.1.8. ∎

Lemma 2.1.10 *The number of Singer cycles in a symplectic group $Sp_{2d}(q)$ is*

$$\frac{1}{2d}q^{2d^2}\left(1-\frac{1}{q^d}\right)\prod_{k=1}^{d-1}\left(1-\frac{1}{q^{2k}}\right).$$

The number of Singer cycles in a general unitary group $GU_d(q^2)$ of odd degree is

$$\frac{1}{d}q^{d(d-1)}\prod_{k=1}^{d-1}\left(1-\frac{(-1)^k}{q^k}\right).$$

In both cases, the Singer cycles are all conjugate to each other.

Proof: As usual, let V be a vector space of dimension d over $\mathbf{F}_q$, let B be a non-singular symplectic or unitary form on V and let $I(V,B)$ be the isometry group of (V,B). If B is symplectic, let $d=2e$ and if B is unitary, we assume that d is odd and $q=q_1^2$. And as before, let τ denote the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_q}(V)$ such that $B(u\varphi,v)=B(u,\tau(\varphi))$ for all $u,v\in V$ and $\varphi\in\mathrm{End}_{\mathbf{F}_q}(V)$.

First we will show that any two Singer cycles in $I(V,B)$ are conjugate. Let $S_1=\langle s_1\rangle$, $S_2=\langle s_2\rangle$ be two Singer cycles in $I(V,B)$ and let $E_1=\mathrm{End}_{\mathbf{F}_qS_1}(V)$, $E_2=\mathrm{End}_{\mathbf{F}_qS_2}(V)$. By Lemma 2.1.4, E_1 and E_2 are fields of cardinality q^d, so $E_1^*=E_1\setminus\{0\}$ and $E_2^*=E_2\setminus\{0\}$ are Singer cycles in $\mathrm{GL}(V)$. We know from the proof of Lemma 2.1.8 that any two Singer cycles in $\mathrm{GL}(V)$ are conjugate, so $g^{-1}E_1^*g=E_2^*$ for some $g\in\mathrm{GL}(V)$. Then of course $g^{-1}S_1g=S_2$ because S_1 and S_2 are the only subgroups of order $q^{\frac{d}{2}}+1$ in E_1^* and in E_2^*, respectively. We may choose the generator elements s_1 and s_2 for S_1 and S_2 so that $g^{-1}s_1g=s_2$. Then since $s_1,s_2\in I(V,B)$,

$$s_2=\tau(s_2)^{-1}=\tau(g^{-1}s_1g)^{-1}=\tau(g^{-1}s_1^{-1}g)=\tau(g)s_1\tau(g)^{-1}$$

so both the conjugation by g and the conjugation by $\tau(g)^{-1}$ take s_1 to s_2, therefore $g\tau(g)\in C_{\mathrm{GL}(V)}(S_1)=E_1^*$. Now we can use the same argument as in the proof of Lemma 2.1.7 to conclude that $g\tau(g)=z\tau(z)$ for some $z\in E_1^*$. (And in general it is always true in a finite field that an element fixed by an involutionary automorphism τ is of the form $z\tau(z)$ for some z in the field.) Now

$$(z^{-1}g)\tau(z^{-1}g)=z^{-1}[g\tau(g)]\tau(z)^{-1}=z^{-1}[z\tau(z)]\tau(z)^{-1}=1\ ,$$

that is, $z^{-1}g\in I(V,B)$. Also, the conjugation by $z^{-1}g$ puts s_1 to s_2, showing that S_1 and S_2 are conjugate in $I(V,B)$.

By Lemma 2.1.2, the set of Singer cycles in $I(V,B)$ is non-empty and by Lemma 2.1.7 the order of the normalizer of a Singer cycle in $I(V,B)$ is $d(q^{\frac{d}{2}}+1)$. Hence the number of Singer cycles in $I(V,B)$ is

$$\frac{|I(V,B)|}{d(q^{\frac{d}{2}}+1)} = \begin{cases} \frac{1}{d(q^{\frac{d}{2}}+1)} q^{\frac{d(d+1)}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1-\frac{1}{q^{2k}}\right), & \text{if } B \text{ is symplectic ;} \\ \frac{1}{d(q^{\frac{d}{2}}+1)} q_1^{d^2} \prod_{k=1}^{d} \left(1-\frac{(-1)^k}{q_1^k}\right), & \text{if } B \text{ is unitary .} \end{cases}$$

$$= \begin{cases} \frac{1}{2e} q^{2e^2} \left(1-\frac{1}{q^e}\right) \prod_{k=1}^{e-1} \left(1-\frac{1}{q^{2k}}\right), & \text{if } B \text{ is symplectic ;} \\ \frac{1}{d} q_1^{d(d-1)} \prod_{k=1}^{d-1} \left(1-\frac{(-1)^k}{q_1^k}\right), & \text{if } B \text{ is unitary .} \end{cases}$$

as wanted. ■

We end this section by proving that the largest cyclic subgroups in a general linear group $\mathrm{GL}_d(q)$ are the Singer cycles. In order to do that, first we prove an interesting fact about polynomials over finite fields.

Lemma 2.1.11 *Let $f(x) \in \mathbf{F}_q[x]$ be a polynomial over $\mathbf{F}_q$ of degree d with $f(0) \neq 0$. Then there is a positive integer r such that $r \leq q^d - 1$ and $f(x)$ divides $x^r - 1$.*

Proof: Use induction on the number of irreducible components of $f(x)$. First assume that $f(x)$ is irreducible over $\mathbf{F}_q$. Then $\mathbf{F}_q[x]/(f(x))$ is a field of cardinality q^d and therefore $x^{q^d-1} \equiv 1$ (modulo $f(x)$).

Next assume that $f(x) = g(x)^k$, $k \geq 2$ and $g(x)$ is an irreducible polynomial over $\mathbf{F}_q$ of degree m. By the previous argument $g(x)$ divides $x^{q^m-1} - 1$. If $k = 2$ then $f(x)$ divides $(x^{q^m-1}-1)^q = x^{q^{m+1}-q} - 1$ while $q^{m+1} - q < q^{km} - 1 = q^d - 1$, so the statement of the lemma is true for $f(x)$. If $k \geq 3$ then $q^{b-1} \leq k < q^b$ for some positive integer b and notice that

$$kq < 1 + q^m + q^{2m} + \ldots + q^{(k-1)m} = \frac{q^{km}-1}{q^m-1} .$$

Then $f(x)$ divides $(x^{q^m-1}-1)^{q^b} = x^{(q^m-1)q^b} - 1$ while

$$(q^m-1)q^b \leq (q^m-1)kq < (q^m-1)\frac{q^{km}-1}{q^m-1} = q^{km} - 1 = q^d - 1 .$$

Finally, assume that $f(x) = g(x)h(x)$ with $(g(x), h(x)) = 1$, deg $g(x) = d_1$, deg $h(x) = d_2$, $g(x)|x^{r_1} - 1$, $h(x)|x^{r_2} - 1$, $r_1 \leq q^{d_1} - 1$ and $r_2 \leq q^{d_2} - 1$. Then $g(x)$ and $h(x)$ both divide $x^{r_1 r_2} - 1$, so $f(x)$ divides $x^{r_1 r_2} - 1$, and $r_1 r_2 \leq (q^{d_1} - 1)(q^{d_2} - 1) \leq q^{d_1 + d_2} - 1 = q^d - 1$. This completes the proof. ■

Lemma 2.1.12 *Let* $\varphi \in GL_d(q)$ *then* $|\varphi| \leq q^d - 1$.

Proof: Let $g(x)$ be the characteristic polynomial of φ. Then deg $g(x) = d$ and by the previous lemma there is a positive integer r such that $r \leq q^d - 1$ and $g(x)$ divides $x^r - 1$. Since $g(\varphi) = 0$, this implies that $\varphi^r - 1 = 0$ and thus the order of φ divides r, a number which is at most $q^d - 1$. ■

2.2 Extension Field Type Subgroups

Lemma 2.2.1 *Let* n, d *be positive integers such that* n *divides* d *and let* q *be any prime power. Then* $GL_d(q)$ *contains a subgroup isomorphic to* $GL_{\frac{d}{n}}(q^n)$.

Proof: Consider a vector space V of dimension $\frac{d}{n}$ over $\mathbf{F}_{q^n}$. Then V is also a d-dimensional vector space over $\mathbf{F}_q$. And since every $\mathbf{F}_{q^n}$-linear transformation of V is also an $\mathbf{F}_q$-linear transformation, we have

$$\mathrm{GL}_{\frac{d}{n}}(q^n) \simeq \mathrm{GL}_{\mathbf{F}_{q^n}}(V) < \mathrm{GL}_{\mathbf{F}_q}(V) \simeq \mathrm{GL}_d(q)$$

showing that $\mathrm{GL}_d(q)$ has a subgroup isomorphic to $\mathrm{GL}_{\frac{d}{n}}(q^n)$. ■

Lemma 2.2.2 *Let* $G \simeq GL_d(q)$ *and let* $H_1, H_2 < G$ *with* $H_1 \simeq H_2 \simeq GL_{\frac{d}{n}}(q^n)$. *Suppose* $H_1 \cap H_2$ *contains a Singer cycle of* G. *Then* $H_1 = H_2$.

Proof: Let $G = \mathrm{GL}(V)$ for some vector space V of dimension d over $\mathbf{F}_q$, and let $\langle s \rangle = S$ be a Singer cycle of G contained in $H_1 \cap H_2$. Furthermore, let $C_1 = Z(H_1)$, $C_2 = Z(H_2)$, $F_1 = C_1 \cup \{0|_V\}$ and $F_2 = C_2 \cup \{0|_V\}$. Then $F_1 \simeq F_2 \simeq \mathbf{F}_{q^n}$ and the actions of F_1 and F_2 define two $\mathbf{F}_{q^n}$-vector space structures on V with $H_1 = \mathrm{GL}_{F_1}(V)$

and $H_2 = \mathrm{GL}_{F_2}(V)$. Notice that C_1 and C_2 both centralize S, so by Lemma 2.1.6 (according to which $C_{\mathrm{GL}(V)}(S) = S$) C_1 and C_2 are both subgroups of S. But since S is cyclic and $|C_1| = |C_2|$, we must have $C_1 = C_2$, and then $F_1 = F_2$ and $H_1 = \mathrm{GL}_{F_1}(V) = \mathrm{GL}_{F_2}(V) = H_2$, as wanted. ■

Lemma 2.2.3 *Let $G \simeq GL_d(q)$ and $H_1, H_2 < G$ with $H_1 \simeq H_2 \simeq GL_{\frac{d}{n}}(q^n)$. Then H_1 and H_2 are conjugate in G.*

Proof: Let S_1 and S_2 be Singer cycles in H_1 and H_2, respectively. Then $|S_1| = |S_2| = (q^n)^{\frac{d}{n}} - 1 = q^d - 1$ so actually S_1 and S_2 are both Singer cycles in G. By Lemma 2.1.8, $S_2 = g^{-1}S_1g$ for some $g \in G$, so S_2 is a Singer cycle in both $g^{-1}H_1g$ and H_2, and by the previous lemma $g^{-1}H_1g = H_2$. ■

Lemma 2.2.4 *Let $G \simeq GL_d(q)$ and $GL_{\frac{d}{n}}(q^n) \simeq H < G$. Then $|N_G(H) : H| = n$ and $N_G(H) \simeq \mathbf{Z}_n \ltimes H$.*

Proof: Assume $G = \mathrm{GL}(V)$ for some vector space V of dimension d over $\mathbf{F}_q$. Let $C = Z(H)$, $F = C \cup \{0|_V\}$, so $F \simeq \mathbf{F}_{q^n}$ and $H = \mathrm{GL}_F(V)$. For any $g \in N_G(H)$, the conjugation by g stabilizes C and F, and fixes $\mathbf{F}_q$ (the field of scalar multiplications on V) elementwise, hence this way we get a natural homomorphism Ψ from $N_G(H)$ to $\mathrm{Gal}(F|\mathbf{F}_q)$ with $\ker(\Psi) = N_G(H) \cap \mathrm{End}_F(V) = H$. Since $|\mathrm{Gal}(F|\mathbf{F}_q)| = n$, this shows that $|N_G(H) : H| \leq n$.

For any $\sigma \in \mathrm{Gal}(F|\mathbf{F}_q)$ define a map $\hat{\sigma}$ on V as follows. Let $\{v_1, v_2, \ldots, v_{\frac{d}{n}}\}$ be a fixed basis of V over F and let

$$\begin{aligned}\hat{\sigma} : V &\longrightarrow V \\ \sum_{k=1}^{\frac{d}{n}} v_k\alpha_k &\longmapsto \sum_{k=1}^{\frac{d}{n}} v_k\alpha_k^{\sigma} \qquad (\forall \alpha_1, \alpha_2, \ldots, \alpha_{\frac{d}{n}} \in F).\end{aligned}$$

It is easy to check $\hat{\sigma}$ is an $\mathbf{F}_q$-linear transformation of V. Furthermore, for any $1 \leq k \leq \frac{d}{n}$ and $\alpha, \beta \in F$

$$(v_k\alpha)(\hat{\sigma}^{-1}\beta\hat{\sigma}) = v_k\alpha^{\sigma^{-1}}(\beta\hat{\sigma}) = v_k(\alpha^{\sigma^{-1}}\beta)^{\sigma} = (v_k\alpha)\beta^{\sigma}$$

which implies that $\hat{\sigma} \in N_G(C) = N_G(H)$ and $\Psi(\hat{\sigma}) = \sigma$. This shows that Ψ is an onto map and therefore $|N_G(H) : H| = n$. It is also clear that for any $\sigma_1, \sigma_2 \in \mathrm{Gal}(F|\mathbf{F}_q)$, $\widehat{\sigma_1\sigma_2} = \hat{\sigma}_1\hat{\sigma}_2$, hence for $R = \{\hat{\sigma} \mid \sigma \in \mathrm{Gal}(F|\mathbf{F}_q)\}$ we have $R \simeq \mathrm{Gal}(F|\mathbf{F}_q) \simeq \mathbf{Z}_n$ and $N_G(H) = R \ltimes H$. ∎

Definition 2.2.5 *Let $G \simeq GL_d(q)$, n be a divisor of d and let $GL_{\frac{d}{n}}(q^n) \simeq H < G$. Then $N_G(H)$ is called an* **extension field type subgroup** *of G.*

The action of $\hat{\sigma}$ on H by conjugation where $\langle\hat{\sigma}\rangle = R$ as in Lemma 2.2.4 is called a **Frobenius action** *on H.*

The next Lemma is a preparation for proving that two different subgroups in $\mathrm{GL}_d(q)$ that are isomorphic to $\mathrm{GL}_{\frac{d}{n}}(q^n)$ have different normalizers.

Lemma 2.2.6 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$ and let S be a Singer cycle in G. Suppose n is a divisor of $\gcd(q^d - 1, d)$ and S_1 is a subgroup of S with index n. Then S_1 acts irreducibly on V and $C_G(S_1) = S$.*

Proof: We will assume that $n > 1$, otherwise there is nothing to prove. First we show that n cannot be divisible by a primitive prime divisor of $q^d - 1$. For if r is a prime divisor of n, then r also divides d, so $q^d - 1 = (q^r)^{\frac{d}{r}} - 1 \equiv q^{\frac{d}{r}} - 1 \pmod{r}$, showing that r is certainly not a primitive prime divisor of $q^d - 1$.

Therefore, if $q^d - 1$ has a primitive prime divisor, then that divides the order of S_1, forcing S_1 to act irreducibly on V. If $q^d - 1$ does not have a primitive prime divisor, then either $(d, q) = (6, 2)$ or $d = 2$ and $q + 1$ is a power of 2. Suppose $(d, q) = (6, 2)$. Then $\gcd(q^d - 1, d) = \gcd(63, 6) = 3$ so $n = 3$ and $|S_1| = 21$. Notice that in this case S_1 has three orbits of size 21 on the set $V \setminus \{0\}$, so any S_1-invariant subspace of V must have a cardinality of $21k + 1$ for some $0 \le k \le 3$, which obviously means that V must be irreducible under the action of S_1. Now suppose $d = 2$. Then

$n = 2$ and S_1 has two orbits on $V \setminus \{0\}$, again leaving no chance for a proper invariant subspace.

Finally, since S_1 acts irreducibly on V, by Lemma 2.1.4 $\mathrm{End}_{\mathbf{F}_q S_1}(V) \simeq \mathbf{F}_{q^d}$, so $|\mathrm{End}_{\mathbf{F}_q S_1}(V)| = q^d$ and $|C_G(S_1)| = q^d - 1$. But on the other hand $|S| = q^d - 1$ and $S \leq C_G(S_1)$, therefore S has to be equal to $C_G(S_1)$. ■

Lemma 2.2.7 *Let $G \simeq GL_d(q)$ and $H_1, H_2 < G$ with $H_1 \simeq H_2 \simeq GL_{\frac{d}{n}}(q^n)$ and $H_1 \neq H_2$. Then $N_G(H_1) \cap N_G(H_2)$ contains no Singer cycles. In particular, $N_G(H_1) \neq N_G(H_2)$.*

Proof: Suppose S is a Singer cycle in G that normalizes H_1, and let $S_1 = S \cap H_1$. Since $|N_G(H_1) : H_1| = n$, $|S : S_1|$ must be a divisor of n and then by the previous lemma, $C_G(S_1) = S$. This implies that the centralizer of H_1, $C_G(H_1)$ is contained in S, and then $S \leq C_G(C_G(H_1)) = H_1$. By the same reason, any Singer cycle normalizing H_2 must be contained in H_2.

By Lemma 2.2.2, no Singer cycle of H_2 is contained in H_1. Hence no Singer cycle in $N_G(H_2)$ is contained in $N_G(H_1)$. ■

Lemma 2.2.8 *Let d, n be positive integers with $n | d$. Then the number of extension field type subgroups in $GL_d(q)$ isomorphic to $\mathbf{Z}_n \ltimes GL_{\frac{d}{n}}(q^n)$ is*

$$\frac{1}{n} \cdot \frac{|GL_d(q)|}{|GL_{\frac{d}{n}}(q^n)|} = \frac{1}{n} q^{d^2 - \frac{d^2}{n}} \prod_{\substack{1 \leq k \leq d \\ n \nmid k}} \left(1 - \frac{1}{q^k}\right).$$

Proof: By Lemma 2.2.3 any two extension field type subgroups corresponding to the same divisor n of d are conjugate in $\mathrm{GL}_d(q)$ and hence the statement follows from Lemma 2.2.4 once we recall that $H_1, H_2 < \mathrm{GL}_d(q)$, $H_1 \simeq H_2 \simeq \mathrm{GL}_{\frac{d}{n}}(q^n)$ and $H_1 \neq H_2$ implies $N_G(H_1) \neq N_G(H_2)$. ■

Lemma 2.2.9 *Suppose V is a vector space of dimension d over $\mathbf{F}_q$, B is a non-singular symplectic form on V and $I(V,B)$ is the isometry group of (V,B). Furthermore, let H be a subgroup of $GL(V)$ isomorphic to $GL_{\frac{d}{n}}(q^n)$ for some divisor n of d and let $H_1 = H \cap I(V,B)$. If H_1 contains a Singer cycle of $I(V,B)$ then*

- *either $H_1 \simeq Sp_{\frac{d}{n}}(q^n)$,*
- *or n is even, $\frac{d}{n}$ is odd and $H_1 \simeq GU_{\frac{d}{n}}(q^n)$.*

Proof: Let $C = Z(H)$, $F = C \cup \{0|_V\}$, so $F \simeq \mathbf{F}_{q^n}$ and $H = \mathrm{GL}_F(V)$, and let τ be the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_q}(V)$ with the property that $B(v\varphi, w) = B(v, w\tau(\varphi))$ for all $v, w \in V$ and $\varphi \in \mathrm{End}_{\mathbf{F}_q}(V)$. Furthermore, let $\langle s_1 \rangle = S_1$ be a Singer cycle of $I(V,B)$ contained in H_1 and let $E = \mathrm{End}_{FS_1}(V) = \mathrm{End}_{\mathbf{F}_q S_1}(V)$, $\langle s \rangle = S = E \setminus \{0\}$, so $E \simeq \mathbf{F}_{q^d}$, S is a Singer cycle in $\mathrm{GL}(V)$ and also in H, and $S \cap I(V,B) = S_1$. Notice that F is a subfield of E since $F \setminus \{0\} = C \leq S = E \setminus \{0\}$.

Now since τ stabilizes S_1 (as $\tau(s_1) = s_1^{-1}$), τ must stabilize $E = \mathrm{End}_{\mathbf{F}_q S_1}(V)$ and therefore every subfield of E, in particular τ stabilizes F. But then τ also stabilizes $\mathrm{End}_F(V)$ and $H = \mathrm{GL}_F(V)$.

Since τ fixes $\mathbf{F}_q$ (the scalar multiplications on V) elementwise, we have that τ acts as a Galois automorphism of the field extension $F|\mathbf{F}_q$. And since $\tau^2 = 1$ and $|\mathrm{Gal}(F|\mathbf{F}_q)| = |\mathrm{Gal}(\mathbf{F}_{q^n}|\mathbf{F}_q)| = n$, τ must be the identity on F whenever n is an odd number. If n is even then τ may act on F as the involutionary field automorphism, in which case $\tau(\alpha) = \alpha^{q^{\frac{n}{2}}}$ for all $\alpha \in F$.

First suppose $\tau(\alpha) = \alpha$ for all $\alpha \in F$ and define an F-bilinear map B_1 on V as follows.

$$\begin{aligned} B_1 : V \times V &\longrightarrow F \\ (u, v) &\longmapsto \sum_{\lambda \in F^*} B(u\lambda^{-1}, v)\lambda \,. \end{aligned}$$

Clearly B_1 is additive in both variables. Furthermore, for any $u, v \in V$ and $\mu \in F$

$$B_1(u\mu, v) = \sum_{\lambda \in F^*} B(u\mu\lambda^{-1}, v)\lambda = \sum_{\lambda \in F^*} B(u(\lambda\mu^{-1})^{-1}, v)(\lambda\mu^{-1})\mu = B_1(u, v)\mu \ ,$$

$$B(v, u) = \sum_{\lambda \in F^*} (v\lambda^{-1}, u)\lambda = \sum_{\lambda \in F^*} -B(u, v\lambda^{-1})\lambda =$$

$$= -\sum_{\lambda \in F^*} B(u\tau(\lambda^{-1}), v)\lambda = -\sum_{\lambda \in F^*} B(u\lambda^{-1}, v)\lambda = -B_1(u, v) \ ,$$

and if Tr denotes the trace map from F to $\mathbf{F}_q$ then

$$\begin{aligned}
\mathrm{Tr}(B_1(u, v)) &= \sum_{\lambda \in F^*} B(u\lambda^{-1}, v)\mathrm{Tr}(\lambda) \\
&= \sum_{\lambda \in F^*} B(u\lambda^{-1}\mathrm{Tr}(\lambda), v) \\
&= B\big(u \sum_{\lambda \in F^*} \lambda^{-1} Tr(\lambda), v\big) \\
&= B\big(u \sum_{\lambda \in F^*} \sum_{k=0}^{n-1} \lambda^{q^k - 1}, v\big) \\
&= B\big(u \sum_{k=0}^{n-1} \sum_{\lambda \in F^*} \lambda^{q^k - 1}, v\big) \\
&= B(-u, v) = -B(u, v)
\end{aligned}$$

because

$$\sum_{\lambda \in F^*} \lambda^t = \begin{cases} -1, & \text{if } |F| - 1 \text{ divides } t \ ; \\ 0, & \text{otherwise} \ . \end{cases}$$

This shows that B_1 is a non-singular symplectic F-bilinear form on V. Let $I(V, B_1) \leq \mathrm{GL}_F(V)$ be the isometry group of (V, B_1). The equality $\mathrm{Tr}(B_1(u, v)) = -B(u, v)$ implies that $I(V, B_1) \leq I(V, B)$, so

$$I(V, B_1) \leq I(V, B) \cap \mathrm{GL}_F(V) = I(V, B) \cap H = H_1 \ .$$

On the other hand if $g \in H_1$ then $g\lambda = \lambda g$ for all $\lambda \in F$ and

$$\begin{aligned} B_1(ug, vg) &= \sum_{\lambda \in F^*} B(ug\lambda^{-1}, vg)\lambda \\ &= \sum_{\lambda \in F^*} B(u\lambda^{-1}g, vg)\lambda \\ &= \sum_{\lambda \in F^*} B(u\lambda^{-1}, v)\lambda \\ &= B_1(u, v) \end{aligned}$$

for all $u, v \in V$. Hence $H_1 = I(V, B_1) \simeq \mathrm{Sp}_{\frac{d}{n}}(q^n)$.

Now suppose $n = 2m$, $F \simeq \mathbf{F}_{q^{2m}}$ and $\tau(\alpha) = \alpha^{q^m}$ for all $\alpha \in F$. Fix an element $\delta \in F$ such that $\delta^{q^m} = -\delta$, let B_1 be the form on V defined as in the previous case and let $B_2(u, v) = \delta B_1(u, v)$ for all $u, v \in V$. Then B_2 is non-singular and linear in the first variable, as we already proved these properties for B_1. Furthermore, for any vectors u, v in V

$$B_2(v, u) = \delta \sum_{\lambda \in F^*} B(v\lambda^{-1}, u)\lambda = \delta \sum_{\lambda \in F^*} -B(u, v\lambda^{-1})\lambda = -\delta \sum_{\lambda \in F^*} B(u\tau(\lambda)^{-1}, v)\lambda =$$

$$= \delta^{q^m} \sum_{\lambda \in F^*} B(u\lambda^{-q^m}, v)\lambda = \delta^{q^m} \sum_{\lambda \in F^*} B(u\lambda^{-1}, v)\lambda^{q^m} = \delta^{q^m} B_1(u, v)^{q^m} = B_2(u, v)^{q^m}.$$

This shows that B_2 is a unitary form on V, and with the same line of reasoning as we did in the previous case, $H_1 = I(V, B_2) \simeq \mathrm{GU}_{\frac{d}{n}}(q^n)$. Notice that in this case $\frac{d}{n}$ must be an odd number, since unitary groups in even dimension do not contain Singer cycles. (See the remark after Lemma 2.1.2.) On the other hand if n is even and $\frac{d}{n}$ is odd, then there is no $\mathrm{Sp}_{\frac{d}{n}}(q^n)$, so H_1 must be isomorphic to $\mathrm{GU}_{\frac{d}{n}}(q^n)$. ∎

Lemma 2.2.10 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$ and let $H_1, H_2 < G$ with $H_1 \simeq H_2 \simeq GL_{\frac{d}{n}}(q^n)$. Furthermore, let B be a non-singular symplectic form on V and let $I(V, B)$ be the isometry group of (V, B). Suppose $H_1 \cap H_2$ contains a Singer cycle of $I(V, B)$. Then $H_1 = H_2$.*

Proof: Let S be a Singer cycle of $I(V, B)$ contained in both H_1 and in H_2 and let $F_1 = Z(H_1) \cup \{0|_V\}$, $F_2 = Z(H_2) \cup \{0|_V\}$. Then $|S| = q^{\frac{d}{2}} + 1$, $F_1 \simeq F_2 \simeq \mathbf{F}_{q^n}$ and by

Lemma 2.1.4,

$$\mathrm{End}_{F_1 S_1}(V) \simeq \mathrm{End}_{F_2 S_1}(V) \simeq \mathrm{End}_{\mathbf{F}_q S_1}(V) \simeq \mathbf{F}_{q^d} .$$

Since obviously $\mathrm{End}_{F_1 S_1}(V) \leq \mathrm{End}_{\mathbf{F}_q S_1}(V)$ and $\mathrm{End}_{F_2 S_1}(V) \leq \mathrm{End}_{\mathbf{F}_q S_1}(V)$, this implies that

$$\mathrm{End}_{F_1 S_1}(V) = \mathrm{End}_{F_2 S_1}(V) = \mathrm{End}_{\mathbf{F}_q S_1}(V)$$

and $S = \mathrm{End}_{\mathbf{F}_q S_1}(V) \setminus \{0\}$ is a Singer cycle not only in G but also in H_1 and H_2. Then by Lemma 2.2.2, $H_1 = H_2$. ■

Lemma 2.2.11 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$ and let $H_1, H_2 < G$ with $H_1 \simeq H_2 \simeq GL_{\frac{d}{n}}(q^n)$. Furthermore, let B be a non-singular symplectic form on V and let $I(V, B)$ be the isometry group of (V, B). Suppose both H_1 and H_2 contain a Singer cycle of $I(V, B)$. Then $H_1 \cap I(V, B)$ and $H_2 \cap I(V, B)$ are conjugate subgroups in $I(V, B)$.*

Proof: Let S_1 and S_2 be Singer cycles of $I(V, B)$ contained in H_1 and in H_2, respectively. By Lemma 2.1.10, $g^{-1}S_1g = S_2$ for some $g \in I(V, B)$. Then S_2 is contained in both $g^{-1}H_1g$ and H_2, so by the previous lemma $g^{-1}H_1g = H_2$ and therefore $g^{-1}[H_1 \cap I(V, B)]g = H_2 \cap I(V, B)$. ■

Lemma 2.2.12 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$ and let $GL_{\frac{d}{n}}(q^n) \simeq H < G$. Furthermore, let B be a non-singular symplectic form on V, $I(V, B)$ the isometry group of (V, B) and $H_1 = H \cap I(V, B)$. If H_1 contains a Singer cycle of $I(V, B)$ then*

$$N_{I(V,B)}(H_1) = N_G(H) \cap I(V, B) .$$

Proof: If $g \in N_G(H) \cap I(V, B)$ then

$$g^{-1}H_1g = g^{-1}(H \cap I(V, B))g = g^{-1}Hg \cap g^{-1}I(V, B)g = H \cap I(V, B) = H_1$$

showing that $N_G(H) \cap I(V,B) \leq N_{I(V,B)}(H_1)$. On the other hand, suppose that $g \in N_{I(V,B)}(H_1)$. Then $H_1 \leq H \cap g^{-1}Hg$ and so H and $g^{-1}Hg$ share some Singer cycles of $I(V,B)$, so by Lemma 2.2.10, $g^{-1}Hg = H$. This shows that $N_{I(V,B)}(H_1) \leq N_G(H)$, therefore $N_{I(V,B)}(H_1) \leq N_G(H) \cap I(V,B)$. ■

Lemma 2.2.13 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$ and let $GL_{\frac{d}{n}}(q^n) \simeq H < G$. Furthermore, let B be a non-singular symplectic form on V, $I(V,B)$ the isometry group of (V,B) and $H_1 = H \cap I(V,B)$. If H_1 contains a Singer cycle of $I(V,B)$ then $|N_{I(V,B)}(H_1) : H_1| = n$. Furthermore, if $\frac{d}{n}$ is even, then*

$$N_{I(V,B)}(H_1) \simeq \mathbf{Z}_n \ltimes H_1 \ .$$

Proof: Define the field F and the map $\Psi : N_G(H) \to \mathrm{Gal}(F|\mathbf{F}_q)$ the same way as in the proof of Lemma 2.2.4. That is, $F = Z(H) \cup \{0|_V\} \simeq \mathbf{F}_{q^n}$ and $\Psi(g)$ is the action of g on F by conjugation for any $g \in N_G(H)$. Let Ψ_1 be the restriction of Ψ to $N_{I(V,B)}(H_1)$. Notice that this restriction does make sense because $N_{I(V,B)}(H_1) \leq N_G(H)$ as we proved it in Lemma 2.2.12. Furthermore,

$$\ker(\Psi_1) = \ker(\Psi) \cap N_{I(V,B)}(H_1) = H \cap (N_G(H) \cap I(V,B)) = H_1 \ ,$$

showing that $N_{I(V,B)}(H_1)/H_1$ is isomorphic to a subgroup of $\mathrm{Gal}(F|\mathbf{F}_q) \simeq \mathbf{Z}_n$.

On the other hand, it is possible to show by an easy calculation that the index of H_1 in $N_{I(V,B)}(H_1)$ is at least n. For if S_1 is a Singer cycle of $I(V,B)$ contained in H_1, then $|N_{I(V,B)}(S_1) : S_1| = d$ and $|N_{I(V,B)}(S_1) \cap H_1 : S_1| = |N_{H_1}(S_1) : S_1| = \frac{d}{n}$. Notice that $N_{I(V,B)}(S_1) \leq N_{I(V,B)}(H_1)$ because of Lemma 2.2.2 and now the image if $|N_{I(V,B)}(S_1)$ in the quotient group $N_{I(V,B)}(H_1)/H_1$ is a cyclic group of order n.

From now, we assume that $\frac{d}{n}$ is even, so $H_1 \simeq \mathrm{Sp}_{\frac{d}{n}}(q^n)$. Define the form B_1 as in the proof of Lemma 2.2.9, so $H_1 = I(V,B_1) \simeq \mathrm{Sp}_{\frac{d}{n}}(q^n)$ if $\frac{d}{n}$ is even and $H_1 = I(V,B_2) \simeq \mathrm{GU}_{\frac{d}{n}}(q^n)$ if $\frac{d}{n}$ is odd. And for any $\sigma \in \mathrm{Gal}(F|\mathbf{F}_q)$ define the linear transformation $\hat{\sigma}$ on V the same way as in the proof of Lemma 2.2.4, with the extra condition that this time let $\{v_1, v_2, \dots, v_{\frac{d}{n}}\}$ be a fixed F-basis of V such that $B_1(v_i, v_j) \in \{-1, 0, 1\}$ for all $1 \leq i, j \leq \frac{d}{n}$. We will show that $\hat{\sigma} \in N_{I(V,B)}(H_1)$ and $\Psi_1(\hat{\sigma}) = \sigma$ for all $\sigma \in \mathrm{Gal}(F|\mathbf{F}_q)$. Actually in Lemma 2.2.4 we proved that $\hat{\sigma} \in N_G(H)$ and $\Psi(\hat{\sigma}) = \sigma$, so what we only need is that $\hat{\sigma} \in I(V, B)$ for any $\sigma \in \mathrm{Gal}(F|\mathbf{F}_q)$.

Let τ be the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_q}(V)$ as in Lemma 2.2.9 and recall that $\tau(\alpha) = \alpha$ for all $\alpha \in F$. Then for any $1 \leq i, j \leq \frac{d}{n}$ and $\alpha, \beta \in F$,

$$B(v_i\alpha\hat{\sigma}, v_j\beta\hat{\sigma}) = B(v_i\alpha^\sigma, v_j\beta^\sigma) =$$

$$= -\mathrm{Tr}\big(B_1(v_i\alpha^\sigma, v_j\beta^\sigma)\big) = -\mathrm{Tr}\big(\alpha^\sigma\tau(\beta^\sigma)B_1(v_i, v_j)\big) = -\mathrm{Tr}\big(\alpha\beta B_1(v_i, v_j)^{\sigma^{-1}}\big) =$$

$$= -\mathrm{Tr}\big(\alpha\tau(\beta)B_1(v_i, v_j)\big) = -\mathrm{Tr}(B_1(v_i\alpha, v_j\beta)) = B(v_i\alpha, v_j\beta)\ .$$

This shows that $\hat{\sigma} \in I(V, B)$ since the set

$$\{v_i\alpha \,|\, 1 \leq i \leq \frac{d}{n}, \alpha \in F\}$$

generates V over $\mathbf{F}_q$.

Finally, since $R = \{\hat{\sigma} \,|\, \sigma \in \mathrm{Gal}(F|\mathbf{F}_q)\}$ is a cyclic group of order n, we have $N_{I(V,B)}(H_1) = R \ltimes H_1 \simeq \mathbf{Z}_n \ltimes H_1$. ∎

Definition 2.2.14 *Let* $G \simeq GL_d(q)$, $Sp_d(q) \simeq G_1 < G$, *let* n *be a divisor of* d *and let* $GL_{\frac{d}{n}}(q^n) \simeq H < G$ *such that* $H_1 = H \cap G_1$ *contains a Singer cycle of* G_1. *Then* $N_{G_1}(H_1)$ *is called an* **extension field type subgroup** *of* G_1.

The action of $\hat{\sigma}$ *on* H_1 *by conjugation, where* $\langle\hat{\sigma}\rangle = R$ *as in Lemma 2.2.13 is called a* **Frobenius action** *on* H_1.

Lemma 2.2.15 *Let* V *be a vector space of dimension* d *over* $\mathbf{F}_q$, $G = GL(V)$ *and let* $H, K < G$ *with* $H \simeq K \simeq GL_{\frac{d}{n}}(q^n)$, $(d, n, q) \notin \{(6, 3, 2), (6, 6, 2), (2, 2, 3)\}$ *and* $H \neq K$. *Furthermore, let* B *be a non-singular symplectic form on* V *and let* $I(V, B)$ *be the isometry group of* (V, B). *Suppose both* $H_1 = H \cap I(V, B)$ *and* $K_1 = K \cap I(V, B)$ *contain a Singer cycle of* $I(V, B)$. *Then* $N_{I(V,B)}(H_1) \cap N_{I(V,B)}(K_1)$ *contains no Singer cycle of* $I(V, B)$.

Proof: Suppose S_1 is a Singer cycle in $I(V, B)$ and $S_1 \leq N_{I(V,B)}(H_1)$. Then let $S = \mathrm{End}_{\mathbf{F}_q S_1}(V) \setminus \{0\}$, so S is a Singer cycle in G. Furthermore, let $C = C_G(H_1)$ and $F = C \cup \{0\}$ so $F \simeq \mathbf{F}_{q^n}$ and $H = \mathrm{GL}_F(V) = C_G(C)$. Since $S_1 \leq N_{I(V,B)}(H_1) \simeq \mathbf{Z}_n \ltimes H_1$, $S_2 = S_1 \cap H_1$ is a subgroup of S_1 such that $|S_1 : S_2|$ divides n.

Now we will show that S_2 must act irreducibly on V. Suppose $q^d - 1$ has a primitive prime divisor r. Then r divides $|S_1| = q^{\frac{d}{2}} + 1$ but does not divide n, for if $r|n$ then $r|d$ and $0 \equiv q^q - 1 = (q^r)^{\frac{d}{r}} - 1 \equiv q^{\frac{d}{r}} - 1 \pmod r$, so r would not be a primitive prime divisor of $q^d - 1$. Therefore, r divides $|S_2|$, forcing S_2 to act irreducibly on V. So S_2 acts irreducibly on V whenever $q^d - 1$ has a primitive prime divisor. Now assume that $q^d - 1$ does not have a primitive prime divisor. Then $(d, q) = (6, 2)$ or $(2, 2^m - 1)$ for some positive integer m. If $(d, q) = (6, 2)$ then because of our assumption in the statement of the lemma $n = 2$, which is coprime to $|S_1| = 9$, so $S_1 = S_2$ and S_1 acts irreducibly on V by Lemma 2.1.3. If $(d, q) = (2, 2^m - 1)$ with $m \geq 3$, then $|S_1| = 2^m$, so $|S_2| = 2^m$ or 2^{m-1}. In both cases S_2 contains a cyclic subgroup of order 4, while there is no cyclic subgroup of order 4 in $\mathrm{GL}_1(q) \times \mathrm{GL}_1(q) \simeq \mathbf{Z}_{2^m-2} \times \mathbf{Z}_{2^m-2}$, therefore S_2 must act irreducibly on V.

Since S_2 has an irreducible action on V, by Lemma 2.1.4, $\mathrm{End}_{\mathbf{F}_q S_2}(V) \simeq \mathbf{F}_{q^d}$. This implies $C_G(S_2) = S$ because $|S| = q^d - 1$ and $S \leq C_G(S_2) = \mathrm{End}_{\mathbf{F}_q S_2}(V) \setminus \{0\}$. But on the other hand, $S_2 \leq H_1$ implies $C \leq C_G(S_2)$. Therefore, $C \leq S$, $S \leq C_G(C) = H$, and $S_1 \leq H \cap I(V, B) = H_1$.

By the same argument, $S_1 \leq N_{I(V,B)}(K_1)$ would imply $S \leq K$, so $S_1 \leq N_{I(V,B)}(H_1) \cap N_{I(V,B)}(H_2)$ would imply $S \leq H \cap K$, which means $H = K$ because of Lemma 2.2.2. ∎

The following lemma is now a straightforward consequence of Lemmas 2.2.11, 2.2.13 and 2.2.15 :

Lemma 2.2.16 *Let d, n be positive integers with d even and $n|d$, and assume that $(d, q) \neq (2, 3)$ and $(d, q) \neq (6, 2)$. Then the number of extension field type subgroups* *in* $Sp_d(q)$ *isomorphic to* $\mathbf{Z}_n \ltimes Sp_{\frac{d}{n}}(q^n)$ *is*

$$\frac{1}{n} \cdot \frac{|Sp_d(q)|}{|Sp_{\frac{d}{n}}(q^n)|} = \frac{1}{n} q^{\frac{d^2}{2} - \frac{d^2}{2n}} \prod_{\substack{1 \leq k \leq d \\ k \text{ even }, 2n \nmid k}} \left(1 - \frac{1}{q^k}\right)$$

if $\frac{d}{n}$ *is an even number, and the number of extension field type subgroups in* $Sp_d(q)$ *isomorphic to* $\mathbf{Z}_n \ltimes GU_{\frac{d}{n}}(q^n)$ *is*

$$\frac{1}{n} \cdot \frac{|Sp_d(q)|}{|GU_{\frac{d}{n}}(q^n)|}$$

if $\frac{d}{n}$ *is an odd number.*

2.3 Maximal Overgroups of Singer Elements

In this section we will obtain a list of maximal subgroups of $\mathrm{SL}_d(q)$ ($q = p^f$, p a prime) containing an element of order $\frac{q^d-1}{q-1}$, and for any odd prime power q and even number d we will obtain a list of maximal subgroups of $\mathrm{Sp}_d(q)$ containing an element of order $q^{\frac{d}{2}} + 1$. Our calculations will be based on a paper by Robert Guralnick, Tim Penttila, Cheryl E. Praeger and Jan Saxl [5]. This paper contains a classification of those subgroups of $\mathrm{GL}_d(q)$ with orders divisible by a primitive prime divisor of $q^e - 1$ for some $\frac{d}{2} < e \leq d$. In particular, this paper has a complete list of the proper subgroups of $\mathrm{GL}_d(q)$ with orders divisible by a primitive prime divisor of $p^{fd} - 1$. Denote the set of these subgroups by $\mathcal{S}(d, q)$.

If M is a maximal subgroup of $\mathrm{GL}_d(q)$ containing an element of order $\frac{q^d-1}{q-1}$ or $q^{\frac{d}{2}} + 1$, and $p^{fd} - 1$ has a primitive prime divisor (that is, $(fd, p) \neq (6, 2)$ and $(fd, p) \neq (2, 2^k - 1)$) then obviously $M \in \mathcal{S}(d, q)$. So we will go through the members of $\mathcal{S}(d, q)$ listed in the paper mentioned above and determine one by one, if they contain an element of order $\frac{q^d-1}{q-1}$ or an element of order $q^{\frac{d}{2}} + 1$ when q is an odd prime power. The cases $(df, p) = (6, 2)$ and $(df, p) = (2, 2^k - 1)$ will have to be handled separately. At certain points we will refer to a paper by W.M. Kantor [6], in which he proves that every maximal overgroup of a Singer element of $\mathrm{GL}_d(q)$ is an extension field type subgroup isomorphic to $\mathrm{GL}_{\frac{d}{r}}(q^r)\cdot r$ for a prime divisor r of d. Throughout this section Z will denote the center of $\mathrm{GL}_d(q)$.

The set $\mathcal{S}(d,q)$ can be broken into a union of four of its subsets the following way.

$$\mathcal{S}(d,q) = \mathcal{S}_1(d,q) \cup \mathcal{S}_2(d,q) \cup \mathcal{S}_3(d,q) \cup \mathcal{S}_4(d,q)\ ,$$

$$\mathcal{S}_1(d,q) = \{G \in \mathcal{S}(d,q) \mid G \text{ has a normal subgroup isomorphic to } \mathrm{SL}_d(q),\ \mathrm{Sp}_d(q),\ \mathrm{SU}_d(q) \text{ or } \Omega_d^{\pm}(q)\ \}$$

$$\mathcal{S}_2(d,q) = \{G \in \mathcal{S}(d,q) \mid G \text{ is a subgroup of a proper extension field type subgroup of } \mathrm{GL}_d(q)\ \}$$

$$\mathcal{S}_3(d,q) = \{G \in \mathcal{S}(d,q) \mid G \leq N_{\mathrm{GL}_d(q)}(S) \text{ for a 2-subgroup } S \text{ of symplectic type of exponent } 4\ \}$$

$$\mathcal{S}_4(d,q) = \{G \in \mathcal{S}(d,q) \mid G \not\leq \mathcal{S}_1(d,q) \cup \mathcal{S}_2(d,q) \cup \mathcal{S}_3(d,q) \text{ and } S \leq G/(G\cap Z) \leq \mathrm{Aut}(S) \text{ for a finite non-abelian simple group } S\ \}\ .$$

If $G \in \mathcal{S}_3(d,q)$ then $d = 2^m$ for some integer $m \geq 1$, $r = d+1$ is a Fermat prime (which implies that m has to be a power of 2), $q = p^f$ with p and f odd and one of the following holds:

1. $d \geq 4$, $p \equiv 1 \pmod 4$ and $G \leq (S\cdot M_0)\circ Z$ with $S \simeq 4\circ 2^{1+2m} = Z_4\circ D_8\circ\ldots\circ D_8$ and $M_0 \simeq \mathrm{Sp}_{2m}(2)$,
2. $G \leq (S\cdot M_0)\circ Z$ with $S \simeq 2_-^{1+2m} = D_8\circ\ldots\circ D_8\circ Q_8$ and $M_0 \simeq \mathrm{O}_{2m}^-(2)$,
3. $d \geq 4$ and $G \leq (S\cdot M_0)\circ Z$ with $S \simeq 2_+^{1+2m} = D_8\circ\ldots\circ D_8$ and $M_0 \simeq \mathrm{O}_{2m}^+(2)$.

If $G \in \mathcal{S}_4(d,q)$ with $d \geq 3$ then $S \leq G/(G \cap Z) \leq \mathrm{Aut}(S)$ for a non-abelian simple group S and one of the following holds:

1. $d = r - 1$ for a prime number $r \geq 5$ such that r is a primitive prime divisor of $q^{r-1} - 1$ and G is isomorphic to a subgroup of $S_{d+2} \times Z_{q-1}$,
2. $d = 3$, $p = 5$ and $S \simeq A_7$,
3. $d = 4$ and $S \simeq A_5$,
4. $d = 4$ and $S \simeq A_6$,
5. $d = 4$ and $S \simeq A_7$,
6. $d = 4$ and $S \simeq A_8$,
7. $d = 6$ and $S \simeq A_7$,
8. $d = 5$ and $S \simeq M_{11}$,
9. $d = 10$ and $S \simeq M_{11}$,
10. $d = 10$ and $S \simeq M_{12}$,
11. $d = 10$ and $S \simeq M_{22}$,
12. $d = 11$ and $S \simeq M_{23}$,
13. $d = 22$ and $S \simeq M_{23}$,
14. $d = 11$ and $S \simeq M_{24}$,
15. $d = 6$, $p \geq 5$ and $S \simeq J_2$,
16. $d = 9$ and $S \simeq J_3$,
17. $d = 18$ and $S \simeq J_3$,

18. $d = 28$ and $S \simeq Ru$,

19. $d = 12$ and $S \simeq Suz$,

20. $d = 6$, $p = 2$ and $S \simeq G_2(q)$,

21. $d = 4$, $p = 2$ and $S \simeq {}^2B_2(q)$,

22. $d = 12$, $p > 2$ and $S \simeq G_2(4)$,

23. $d = 4$, $p \equiv 1 \pmod 6$ and $S \simeq \mathrm{PSU}_4(4) \simeq \mathrm{PSp}_4(3)$,

24. $d = 6$, $p \equiv 1 \pmod 6$ and $S \simeq \mathrm{PSU}_4(9)$,

25. $d = 6$, $p > 2$ and $S \simeq \mathrm{PSL}_3(4)$,

26. $d = \frac{s^n-1}{s-1} - 1$ for some prime power s coprime to q and a prime number $n \geq 3$ such that $r = d + 1$ is a prime, and $S \simeq \mathrm{PSL}_n(s)$,

27. $d = \frac{s^n+1}{s+1} - 1$ for some prime power s coprime to q and a prime number $n \geq 3$ such that $r = d + 1$ is a prime, and $S \simeq \mathrm{PSU}_n(s^2)$,

28. $d = \frac{s^n-1}{2}$ with s an odd prime power, coprime to q and $n = 2^b \geq 2$ such that $r = d + 1$ is a prime, and $S \simeq \mathrm{PSp}_{2n}(s)$,

29. $d = 2^c$, $c = 2^{c'} \geq 4$ such that $r = d + 1$ is a prime, q is odd and $S \simeq \mathrm{PSL}_2(d)$,

30. $d \geq 6$, $d + 1$ is a prime and $S \simeq \mathrm{PSL}_2(d + 1)$,

31. $d \geq 3$, $2d + 1$ is a prime power and $S \simeq \mathrm{PSL}_2(2d + 1)$,

We should mention that in most of these cases there are additional conditions for q or d, but for simplicity reasons we will not consider them, as long as it is not necessary for our calculations.

Theorem 2.3.1 *Suppose $d = 2^m \geq 4$, $q = p^f$ with p, f odd, $G \in \mathcal{S}_3(d,q)$ and G contains an element of order $q^{\frac{d}{2}} + 1$. Then $(d,q) = (4,3)$.*

Proof: Since $G \in \mathcal{S}_3(d,q)$, $G \leq M = (S \cdot M_0) \circ Z$ with $S \simeq Z_4 \circ \underbrace{D_8 \circ \ldots \circ D_8}_{m}$, $M_0 \simeq \mathrm{Sp}_{2m}(2)$, or $S \simeq \underbrace{D_8 \circ \ldots \circ D_8}_{m-1} \circ Q_8$ and $M_0 \simeq \mathrm{O}^-_{2m}(2)$, or $S \simeq \underbrace{D_8 \circ \ldots \circ D_8}_{m}$ and $M_0 \simeq \mathrm{O}^+_{2m}(2)$. Then $S \cdot M_0$ contains an element of order $\frac{1}{2}(q^{\frac{d}{2}} + 1)$, since $\gcd(q^{\frac{d}{2}} + 1, |Z|) = 2$. On the other hand, the largest element orders in S and M_0 are less than or equal to 8 and $2^{2m} - 1$, respectively, therefore $\frac{1}{2}(q^{\frac{d}{2}} + 1) \leq 8(2^{2m} - 1)$, $q^{\frac{d}{2}} < 2^{2m+4}$, $q^d < 2^{4m+8}$. Since q is odd, we must have $3^d < 2^{4m+8}$, so $2^m = d < (4m+8)\log_3 2 < (4m+8)\frac{2}{3}$, which implies $m < 4$. Since m is a power of 2 itself, it follows that $m = 2$ and $d = 4$. Now $q^{\frac{d}{2}} + 1 = q^2 + 1$ must divide $|S| \cdot |M_0| \cdot |Z|$, which divides $2^{2m+2}|\mathrm{Sp}_{2m}(2)|(q-1) = 2^{10} \cdot 3^2 \cdot 5 \cdot (q-1)$. Since $\gcd(q^2+1, 2^{10}(q-1)) = 2$ we have that $q^2 + 1$ divides $2 \cdot 3^2 \cdot 5 = 90$. The only solution for this is $q = 3$, in which case $(d,q) = (4,3)$. ■

Before we start studying the groups in $\mathcal{S}_4(d,q)$, we prove a little lemma about the automorphism groups of finite PSL_2 groups.

Lemma 2.3.2 *If p is any prime number and $q = p^f \geq 5$ then the largest element order in $Aut(PSL_2(q))$ is $q + 1$.*

Proof: It is well known that

$$\mathrm{Aut}(\mathrm{PSL}_2(q)) \simeq \mathrm{P\Gamma L}_2(q) \simeq [\mathrm{Aut}(\mathbf{F}_q) \ltimes \mathrm{GL}_2(q)]/Z$$

where $Z = Z(\mathrm{GL}_2(q))$ and the action of $\mathrm{Aut}(\mathbf{F}_q)$ on $\mathrm{GL}_2(q)$ is understood in the natural way.

Let $(\sigma, A) \in \mathrm{Aut}(\mathbf{F}_q) \ltimes \mathrm{GL}_2(q)$ with σ having order k in $\mathrm{Aut}(\mathbf{F}_q)$. Then

$$(\sigma, A)^k = (1, A^{\sigma^{k-1}} \cdot \ldots A^{\sigma} \cdot A) = (1, B)$$

with $A^{-1}BA = B^{\sigma}$. This implies that the characteristic polynomial of B has all of its coefficients in $F = \{\alpha \in \mathbf{F}_q \mid \alpha^{\sigma} = \alpha\}$, which is a subfield of $\mathbf{F}_q$ with $|\mathbf{F}_q : F| = k$. So if $F \simeq \mathbf{F}_{q_1}$ then $q = q_1^k$. There are three possibilities for B.

1. B represents a p-element in $\mathrm{PGL}_2(q)$;
2. B is a p'-element in $\mathrm{GL}_2(q)$ and the characteristic polynomial of B is reducible over F;
3. B is a p'-element in $\mathrm{GL}_2(q)$ and the characteristic polynomial of B does not factor over F.

In case 1, the order of B in $\mathrm{PGL}_2(q)$ is p and therefore $(\sigma, A)^{kp} \in Z$. In case 2, B is diagonalizable over F and therefore $(\sigma, A)^{k(q_1-1)} = 1$. In case 3, B has two roots α and β in $\mathbf{F}_{q_1^2}$ such that $\alpha^{q_1+1} = \beta^{q_1+1}$ and therefore $(\sigma, A)^{k(q_1+1)} \in Z$. This shows that the order of (σ, A) modulo Z is less than or equal to $k(q_1+1)$. We need to show that $k(q_1+1) \leq q+1 = q_1^k + 1$. Notice that

$$\frac{q_1^k+1}{q_1+1} \geq \frac{2^k+1}{3} \quad \text{and} \quad \frac{2^k+1}{3} \geq k$$

whenever $k \neq 2$. If $k = 2$ then $2(q_1+1) \leq q_1^2 + 1$ unless $q_1 = 2$ in which case $q = 4$.

In fact, $\mathrm{Aut}(\mathrm{PSL}_2(q))$ always contains an element of order $q+1$, since the image of a Singer cycle of $\mathrm{GL}_2(q)$ in $\mathrm{PGL}_2(q)$ is always of order $q+1$. ■

Theorem 2.3.3 *Suppose $d \geq 3$, $G \in \mathcal{S}_4(d,q)$, and one of the following holds:*

- *G contains an element of order $\frac{q^d-1}{q-1}$;*
- *d is even, q is odd and G contains an element of order $q^{\frac{d}{2}} + 1$.*

Then $(d,q) = (3,4)$ in the first case, and $(d,q) = (4,3)$ or $(6,3)$ in the second case.

Proof: *Case 1:* Assume that $d = r - 1$ for a prime number $r \geq 5$ such that r is a primitive prime divisor of $q^{r-1} - 1$ and G is isomorphic to a subgroup of $S_{d+2} \times Z_{q-1}$.

Notice that in this case d is even and $d \geq 4$. Since r is coprime to $(q-1)$, every element in $S_{d+2} \times Z_{q-1}$ with order divisible by r must be of the form (σ, t) with some r-cycle σ in S_{d+2}. Then $|(\sigma, t)|$ divides $r(q-1)$. Now since r divides $q^{\frac{d}{2}}+1$ and by our assumption G has an element of order $q^{\frac{d}{2}}+1$, it follows that $q^{\frac{d}{2}}+1$ divides $r(q-1)$. And since $\gcd(q^{\frac{d}{2}}+1, q-1) = \gcd(q-1, 2)$, $q^{\frac{d}{2}}+1$ divides $\gcd(q-1,2)r = \gcd(q-1,2)(d+1)$. This cannot happen if $q \geq 4$ because $4^{\frac{d}{2}} + 1 = 2^d + 1 > 2(d+1)$ for all $d \geq 4$. If $q = 3$ then d must be 4 (otherwise $3^{\frac{d}{2}} + 1 > 2(d+1)$), so $(d, q) = (4, 3)$. If $q = 2$ then actually $\frac{q^d-1}{q-1} = 2^d - 1$ divides $\gcd(q-1, 2)r = r = d+1$, which cannot happen for any $d \geq 4$.

In all of the following cases we will use that $G/(G \cap Z) \leq \mathrm{Aut}(S)$ for a finite non-abelian simple group S. This always implies that if G has an element of order $\frac{q^d-1}{q-1}$ then $\mathrm{Aut}(S)$ must have an element of order $\frac{q^d-1}{\gcd(q-1,d)(q-1)}$ and if G has an element of order $q^{\frac{d}{2}}+1$ then $\mathrm{Aut}(S)$ must have an element of order $\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1)$. This is simply because $\gcd(\frac{q^d-1}{q-1}, q-1) = \gcd(q-1, d)$ and $\gcd(q^{\frac{d}{2}}+1, q-1) = \gcd(q-1, 2)$.

Case 2: Assume that $d = 3$, $p = 5$ and $S \simeq A_7$, so $S_7 \simeq \mathrm{Aut}(A_7)$ contains an element of order $\frac{q^3-1}{\gcd(q-1,3)(q-1)} = \frac{1}{\gcd(q-1,3)}(q^2+q+1)$. Since the largest order in S_7 is 12, this implies $q = 2$ or $q = 4$ but neither of them is a power of 5, so this case cannot happen.

Case 3: Assume that $d = 4$ and $S \simeq A_5$, so $S_5 \simeq \mathrm{Aut}(A_5)$ contains an element of order $\frac{1}{2}(q^2+1)$ if q is odd and S_5 contains an element of order $\frac{q^4-1}{q-1} = (q^2+1)(q+1)$ if q is even. This happens only with $q = 3$, so $(d, q) = (4, 3)$, in which case S_5 contains an element of order $\frac{1}{2}(q^2+1) = 5$, but no elements of order $\frac{q^4-1}{\gcd(q-1,4)(q-4)} = 20$.

Case 4: Assume that $d = 4$ and $S \simeq A_6$. Then S_6, which is isomorphic to a subgroup of $\mathrm{Aut}(A_6)$ of index 2 contains an element of order $\frac{1}{2}(q^2+1)$ if q is odd, or an element of order $(q^2+1)(q+1)$ if q is even. (This is because any element with odd order is contained in any subgroup of index 2, in general.) As in the previous case, this implies $(d, q) = (4, 3)$, and since the largest element order in $\mathrm{Aut}(A_6)$ is 10, G cannot contain a Singer cycle of $\mathrm{SL}_4(3)$.

Case 5: Assume that $d = 4$ and $S \simeq A_7$. The same argument goes as for the previous two cases.

Case 6: Assume that $d = 4$ and $S \simeq A_8$. As above, either q is odd and S_8 contains an element of order $\frac{1}{2}(q^2 + 1)$ or q is even and S_8 contains an element of order $(q^2 + 1)(q + 1)$. This time beside $q = 3$, $q = 2$ is also a possibility. This is no surprise, since $\mathrm{GL}_4(2) \simeq A_8$, however, $\mathrm{GL}_4(2)$ is not a member of $\mathcal{S}_4(4, 2)$.

Case 7: Assume that $d = 6$ and $S \simeq A_7$, so S_7 contains an element of order $\frac{1}{2}(q^3 + 1)$ if q is odd, and an element of order $\frac{1}{3}(q^3 + 1)(q^2 + q + 1)$ if q is even. But there is no such prime power q.

Case 8: Assume that $d = 5$ and $S \simeq M_{11}$. Then $M_{11} \simeq \mathrm{Aut}(M_{11})$ should contain an element of order $\frac{q^5-1}{\gcd(q-1,5)(q-1)}$, but on the other hand, the largest element order in M_{11} is 11. So if 5 divides $q - 1$ then $q^5 - 1 \leq 55(q - 1)$ and $q^4 < 55$, and if 5 does not divide $q - 1$ then $q^5 - 1 \leq 11(q - 1)$ and $q^4 < 11$. This is a contradiction in either ways.

Case 9: Assume that $d = 10$ and $S \simeq M_{11}$. Then M_{11} has to contain an element of order $\frac{1}{\gcd(q-1,2)}(q^5 + 1)$, which is not possible, since again, the largest element order in M_{11} is 11 and $\frac{1}{\gcd(q-1,2)}(q^5 + 1)$ is always bigger then that.

Case 10: Assume that $d = 10$ and $S \simeq M_{12}$. As above, this is another impossible case, since the largest element order in $\mathrm{Aut}(M_{12})$ is 12, which is less than $\frac{1}{\gcd(q-1,2)}(q^5 + 1)$ for any prime power q.

Case 11: Assume that $d = 10$ and $S \simeq M_{22}$. The largest element order in M_{22} is 14, and as for the previous two cases, $14 < \frac{1}{\gcd(q-1,2)}(q^5 + 1)$ for any prime power q.

Case 12: Assume that $d = 11$ and $S \simeq M_{23}$. The largest element order in $\mathrm{Aut}(M_{23}) = M_{23}$ is 23, which is certainly less than $\frac{q^{11}-1}{\gcd(q-1,11)(q-1)}$ for any prime power q.

Case 13: Assume that $d = 22$ and $S \simeq M_{23}$. Again, $23 < \frac{1}{\gcd(q-1,2)}(q^{11}+1)$ for any prime power q.

Case 14: Assume that $d = 11$ and $S \simeq M_{24}$. The largest element order in $\mathrm{Aut}(M_{24}) \simeq M_{24}$ is 23, while $G/(G \cap Z)$ should contain an element of order $\frac{q^{11}-1}{\gcd(q-1,11)(q-1)}$ which is bigger than q^9; another contradiction.

Case 15: Assume that $d = 6$, $p \geq 5$ and $S \simeq J_2$, so $\mathrm{Aut}(J_2)$ contains an element of order $\frac{1}{\gcd(q-1,2)}(q^3+1)$. On the other hand, the largest element order in $\mathrm{Aut}(J_2)$ is 24, so $\frac{1}{\gcd(q-1,2)}(q^3+1) \leq 24$, which implies $q \leq 3$, contradicting with the assumption that $p \geq 5$.

Case 16: Assume that $d = 9$ and $S \simeq J_3$, so $\mathrm{Aut}(J_3)$ should contain an element of order $\frac{q^9-1}{\gcd(q-1,9)(q-1)}$, which is bigger than q^7. But this is not possible, since the largest element order in $\mathrm{Aut}(J_3)$ is 34.

Case 17: Assume that $d = 18$ and $S \simeq J_3$, so $\mathrm{Aut}(J_3)$ should contain an element of order $\frac{1}{\gcd(q-1,2)}(q^9-1)$, but this number is always bigger than 34.

Case 18: Assume that $d = 28$ and $S \simeq Ru$. The largest element order in $\mathrm{Aut}(Ru) \simeq Ru$ is 29, which is less than $\frac{1}{\gcd(q-1,2)}(q^{14}+1)$ for any prime power q.

Case 19: Assume that $d = 12$ and $S \simeq Suz$. The largest element order in $\mathrm{Aut}(Suz)$ is 40, which is less than $\frac{1}{\gcd(q-1,2)}(q^6+1)$ for any prime power q, so this is another non-existing case.

Case 20: Assume that $d = 6$, $q = 2^f$ and $S \simeq G_2(q)$. The 6-dimensional representation of $G_2(q)$ considered in this case is a symplectic representation (see B. N. Cooperstein [2] for more details), eliminating the possibility for G to contain a Singer cycle of $\mathrm{GL}_6(q)$.

Case 21: Assume that $d = 4$, $q = 2^f$, f an odd integer and $S \simeq {}^2B_2(q)$. Let r be any primitive prime divisor of $2^{2f}-1$. Then r does not divide f, otherwise $0 \equiv 2^{2f}-1 = (2^r)^{\frac{2f}{r}}-1 \equiv 2^{\frac{2f}{r}}-1 \pmod r$ and r would not be a primitive prime divisor of $p^{2f}-1$. Now, since $|\mathrm{Aut}({}^2B_2(q))| = fq^2(q^2+1)(q-1) = f2^{2f}(2^{2f}+1)(2^f-1)$

is not divisible by r, but r divides $\frac{q^4-1}{\gcd(q-1,4)(q-1)}$, it follows that G cannot contain an element of order q^4-1. In case if $2^{2f}-1$ does not have a primitive prime divisor, then $2^{2f}=64$, $f=3$, $q=8$ and $|\mathrm{Aut(S)}| = 3\cdot 64\cdot 65\cdot 7 = 2^6\cdot 3\cdot 5\cdot 7\cdot 13$, while $\frac{q^4-1}{\gcd(q-1,4)(q-1)} = \frac{8^4-1}{\gcd(7,4)(7)} = 3^2\cdot 5\cdot 13$, so G cannot contain a Singer cycle of $\mathrm{GL}_4(q)$ in this case either.

Case 22: Assume that $d=12$, $p>2$ and $S\simeq G_2(4)$, so $\mathrm{Aut}(G_2(4))$ should contain an element of order $\frac{1}{\gcd(q-1,2)}(q^6+1)$. But this is not possible since the largest element order in $\mathrm{Aut}(G_2(4))$ is 24.

Case 23: Assume that $d=4$, $p\equiv 1 \pmod 6$ and $S\simeq \mathrm{PSU}_4(4)\simeq \mathrm{PSp}_4(3)$, so $\mathrm{Aut}(\mathrm{PSU}_4(2))$ should contain an element of order $\frac{1}{\gcd(q-1,2)}(q^2+1)=\frac{1}{2}(q^2+1)$. This is always at least 25 if $q\equiv 1 \pmod 6$, but on the other hand, the largest element order in $\mathrm{Aut}(\mathrm{PSU}_4(2))$ is 12.

Case 24: Assume that $d=6$, $p\equiv 1 \pmod 6$ and $S\simeq \mathrm{PSU}_4(9)$, and therefore $\mathrm{Aut}(\mathrm{PSU}_4(9))$ should contain an element of order $\frac{1}{\gcd(q-1,2)}(q^3+1)=\frac{1}{2}(q^3+1)$. This is always at least 172 when $q\equiv 1 \pmod 6$, but in fact the largest element order in $\mathrm{Aut}(\mathrm{PSU}_4(9))$ is 28.

Case 25: Assume that $d=6$, $p>2$ and $S\simeq \mathrm{PSL}_3(4)$, so $\mathrm{Aut}(\mathrm{PSL}_3(4))$ should contain an element of order $\frac{1}{\gcd(q-1,2)}(q^3+1)=\frac{1}{2}(q^3+1)$. The largest element order in $\mathrm{Aut}(\mathrm{PSL}_3(4))$ is actually 21, so $q^3+1\leq 42$, $q=3$ and $(d,q)=(6,3)$. Notice that even in the $(d,q)=(6,3)$ case, G cannot contain an element of order $\frac{q^6-1}{q-1}=\frac{3^6-1}{2}=364$ since that would imply the existence of an element of order $\frac{1}{2}\cdot 364 = 182$ in $\mathrm{Aut}(\mathrm{PSL}_3(4))$.

Case 26: Assume that $d=\frac{s^n-1}{s-1}-1$ for some prime power s coprime to q and a prime number $n\geq 3$ such that $r=d+1$ is a prime, and $S\simeq \mathrm{PSL}_n(s)$. In this case d is even, so $G/(G\cap Z)$ contains an element of order $\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1)$. Let $s=a^b$ with a a prime, so the largest element order in $\mathrm{Aut}(\mathrm{PSL}_n(s))$ is less than or equal to $(s^n-1)2b$. (Because the largest element order in $\mathrm{GL}_n(s)$ is s^n-1 and $\mathrm{Aut}(\mathrm{PSL}_n(s))$

has a subgroup of index $2b$ isomorphic to $\mathrm{PGL}_n(s)$.) Hence

$$\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1) \leq (s^n-1)2b \leq (s^n-1)2^b \leq (s^n-1)s\ , \tag{2.1}$$

and $q^{\frac{d}{2}} < 2(s^n-1)s = 2(d+1)(s-1)s < 2(d+1)s^2 < 2(d+1)d$. This implies $2^d < 4(d+1)^2d^2$ and thus $d < 20$. Taking into consideration that $d = \frac{s^n-1}{s-1} - 1$ with s a prime power and n an odd prime, we must have $n = 3$, $d = \frac{s^3-1}{s-1} - 1 = s^2 + s$, so either $s = 2$ and $d = 6$ or $s = 3$ and $d = 12$.

Suppose $s = 3$ and $d = 12$. Then by (2.1), $\frac{1}{\gcd(q-1,2)}(q^6+1) \leq (3^3-1)2 = 54$, a contradiction, since this is not satisfied by any prime power q. Suppose $s = 2$ and $d = 6$. Then $S \simeq \mathrm{PSL}_n(s) = \mathrm{PSL}_3(2)$ and the largest element order in $\mathrm{Aut}(S)$ is 8. Therefore, (2.1) can be replaced by the inequality $\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1) \leq 8$ and there is no solution for this.

Case 27: Assume that $d = \frac{s^n+1}{s+1} - 1$ for some prime power s coprime to q and a prime number $n \geq 3$ such that $r = d+1$ is a prime, and $S \simeq \mathrm{PSU}_n(s^2)$. As in the previous, case d is even, so $G/(G \cap Z)$ contains an element of order $\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1)$, and if $s = a^b$ with a prime then the largest order in $\mathrm{Aut}(\mathrm{PSU}_n(s^2))$ is less than or equal to $(s^{2n}-1)2b$ (because $\mathrm{Aut}(\mathrm{PSU}_n(s^2))$ has a subgroup of index $2b$ isomorphic to a subgroup of $\mathrm{PGL}_n(s^2)$.) Hence

$$\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1) \leq (s^{2n}-1)2b \leq (s^{2n}-1)s\ . \tag{2.2}$$

Suppose q is odd. Then $\frac{1}{2}(q^{\frac{d}{2}}+1) \leq (s^{2n}-1)s$, $q^{\frac{d}{2}} < (s^n+1)^2s = (d+1)^2(s+1)^2s < (d+1)^5$ and $3^{\frac{d}{2}} < (d+1)^5$, which implies $d < 32$. Since $d = \frac{s^n+1}{s+1} - 1 \geq s^{n-1} - s^{n-2} \geq s^{n-2}$, we must have $n \leq 5$ and either $(n,s) = (5,2)$ or $n = 3$. If $n = 5$ and $s = 2$ then $d = 10$ and $S \simeq \mathrm{PSU}_5(4)$ and the largest element order in $\mathrm{Aut}(S)$ is 24, so (2.2) can be replaced by $\frac{1}{2}(q^5+1) \leq 24$, which has no solution for odd prime powers. If $n = 3$ then $d = s^2 - s = s(s-1)$ and (2.2) implies $q^{\frac{s(s-1)}{2}} < 2s(s^6-1) < 2s^7$, $3^{s(s-1)} < 4s^{14}$ and therefore $s \leq 5$. For $s = 5$, $r = d+1 = s(s-1)+1 = 21$ is a contradiction since 21 is not a prime number. If $s = 4$ then $d = 12$, $S \simeq \mathrm{PSU}_3(16)$ and the largest element order in Aut(S) is 16. Hence Aut(S) cannot contain an element of order $\frac{1}{2}(q^{\frac{d}{2}}+1) = \frac{1}{2}(q^6+1)$ for any prime power q. If $s = 3$ then $d = 6$, $S \simeq \mathrm{PSU}_3(9)$, and the largest element order in Aut(S) is 12. Hence Aut(S) cannot contain an element of order $\frac{1}{2}(q^{\frac{d}{2}}+1) = \frac{1}{2}(q^3+1)$ for any odd prime power q. If $s = 2$ then $d = 2$, which case is not considered in this theorem.

Now suppose that q is even. Then $G/(G \cap Z)$ contains an element of order $\frac{q^d-1}{\gcd(q-1,d)(q-1)}$, so (2.2) can be replaced by $\frac{q^d-1}{\gcd(q-1,d)(q-1)} \leq (s^{2n}-1)s$, and therefore $q^{d-2} < (s^n+1)^2 s = (d+1)^2(s+1)^2 s \leq (d+1)^4 d$. This implies $2^{d-2} < (d+1)^5$ and $d < 26$. But since $d = \frac{s^n+1}{s+1} - 1$ for some odd prime power s and an odd prime n, this can only happen if $n = 3$ and $s = 3$ or 5. Again, if $s = 5$ then $r = d+1 = s(s-1)+1 = 21$ is not a prime, and if $s = 3$ then the largest element order in $\mathrm{Aut}(S) = \mathrm{Aut}(\mathrm{PSU}_3(9))$ is 12, which is less than $\frac{q^d-1}{\gcd(q-1,d)(q-1)} = \frac{q^6-1}{\gcd(q-1,6)(q-1)}$ for any prime power q. This concludes the discussion of Case 27.

Case 28: Assume that $d = \frac{s^n-1}{2}$ with s an odd prime power, coprime to q and $n = 2^b \geq 2$ such that $r = d+1$ is a prime, and $S \simeq \mathrm{PSp}_{2n}(s)$. Then $G/(G \cap Z)$ contains an element of order $\frac{1}{\gcd(q-1,2)}(q^{\frac{d}{2}}+1)$, while the largest element order in $\mathrm{Aut}(\mathrm{PSp}_{2n}(s))$ is less than $(s^{2n}-1)s$, therefore

$$q^{\frac{d}{2}} < 2(s^{2n}-1)s < 2s^{2n+1} \tag{2.3}$$

and

$$2^{s^n} = 2^{2d+1} \leq 2q^{2d} < 32s^{8n+4} \leq 32s^{10n} = 32(s^n)^{10} .$$

This implies $s^n < 66$, so $n = 2$ and $s \leq 7$. If $s = 7$ then $d = \frac{7^2-1}{2} = 24$ and $r = d+1 = 25$, which is a contradiction, since 25 is not a prime number. If $s = 5$ then $d = \frac{5^2-1}{2} = 12$, $S \simeq \mathrm{PSp}_4(5)$ and the largest element order in $\mathrm{Aut}(\mathrm{PSp}_4(5))$ is 30. So $\frac{1}{\gcd(q-1,2)}(q^6+1) \leq 30$ and there is no such prime power q. If $s = 3$ then $d = \frac{3^2-1}{2} = 4$, $S \simeq \mathrm{PSp}_4(3)$ and the largest element order in $\mathrm{Aut}(\mathrm{PSp}_4(3))$ is 12. So $\frac{1}{\gcd(q-1,2)}(q^2+1) \leq 12$ if q odd and $\frac{q^4-1}{\gcd(q-1,4)(q-1)} = (q^2+1)(q+1) \leq 12$ if q is even.

The only prime power satisfying this condition is $q = 3$, in which case s would not be coprime to q, contradicting our assumption.

Case 29: Assume that $d = 2^c$, $c = 2^{c'} \geq 4$ such that $r = d + 1$ is a prime, q is odd and $S \simeq \mathrm{PSL}_2(d)$. By Lemma 2.3.2 the largest element order in $\mathrm{Aut}(\mathrm{PSL}_2(d))$ is $d+1$, therefore $\frac{1}{2}(q^{\frac{d}{2}} + 1) \leq d + 1$, $3^{\frac{d}{2}} \leq q^{\frac{d}{2}} < 2(d+1)$. This implies $d \leq 4$, which contradicts to our assumption that $d = 2^c$ with $c \geq 4$.

*Case 30:*Assume that $d \geq 6$, $d+1$ is a prime and $S \simeq \mathrm{PSL}_2(d+1)$. Then the largest element order in $\mathrm{Aut}(S)$ is $d+2$ (again, by Lemma 2.2.3), hence $\frac{1}{2}(q^{\frac{d}{2}} + 1) \leq d + 2$. If $q \geq 3$ then this implies $3^{\frac{d}{2}} < 2d + 4$, contradicting to our assumption that $d \geq 6$. If $q = 2$ then $G/(Z \cap G)$ contains an element of order $2^d - 1$, so $2^d - 1 \leq d + 2$, which is another contradiction.

Case 31: Assume that $d \geq 3$, $2d + 1$ is a prime and $S \simeq \mathrm{PSL}_2(2d + 1)$. Again, by Lemma 2.3.2 the largest element order in $\mathrm{Aut}(S)$ is $2d + 2$. First suppose that d is odd or q is even. Then $G/(Z \cap G)$ has an element of order $\frac{q^d - 1}{\gcd(q-1,d)(q-1)}$ and so $\frac{q^d-1}{\gcd(q-1,d)(q-1)} \leq 2d + 2$. If $q = 2$ then this condition implies $d = 3$, and $S \simeq \mathrm{PSL}_2(7) \simeq \mathrm{PSL}_3(2) = \mathrm{GL}_3(2) = \mathrm{GL}_d(q)$ and thus $G = \mathrm{GL}_3(2)$, contradicting with $G \in \mathcal{S}_4(d, q)$. If $q \geq 3$ then we must have $3^{d-2} \leq q^{d-2} < 2d + 2$, which implies $d \leq 4$. For $d = 3$, $\frac{q^3-1}{\gcd(q-1,3)(q-1)} \leq 2 \cdot 3 + 2 = 8$ must hold, and the only solution for this is $q = 4$, in which case $(d, q) = (3, 4)$. For $d = 4$, $\frac{q^4-1}{\gcd(q-1,4)(q-1)} \leq 2 \cdot 4 + 2 = 10$ must hold, but this has no solution for $q \geq 3$.

Now suppose d is even and q is odd. Then $G/(Z \cap G)$ has an element of order $\frac{1}{2}(q^{\frac{d}{2}} + 1)$, so $3^{\frac{d}{2}} < q^{\frac{d}{2}} + 1 \leq 4d + 4$, therefore $d = 4$ or $d = 6$ and in both cases q must be 3. So $(d, q) = (4, 3)$ or $(d, q) = (6, 3)$. ■

Theorem 2.3.4 *Suppose $G \leq SL_d(q)$ is a maximal overgroup of a Singer cycle of $SL_d(q)$, $d \geq 3$ and $(d, q) \neq (3, 4)$. Then G is the intersection of $SL_d(q)$ with an extension field type subgroup of $GL_d(q)$.*

Proof: Let $q = p^f$ with p a prime. If $p^{fd} - 1$ has a primitive prime divisor, then $G \in \mathcal{S}(d,q)$. If $(d,q) \neq (4,3)$ then by Theorems 2.3.1 and 2.3.3, $G \notin \mathcal{S}_3(d,q) \cup \mathcal{S}_4(d,q)$. Also, $G \notin \mathcal{S}_1(d,q)$, since the orthogonal, symplectic or unitary subgroups of $\mathrm{GL}_d(q)$ do not contain elements of order $\frac{q^d-1}{q-1}$ for $d \geq 3$. Hence $G \in \mathcal{S}_2(d,q)$, which means that G must be the intersection of $\mathrm{SL}_d(q)$ and an extension field type subgroup of $\mathrm{GL}_d(q)$ that is isomorphic to $\mathrm{GL}_{\frac{d}{r}}(q^r) \cdot r$ for some prime divisor r of d. Now suppose $(d,q) = (4,3)$. Then the image of G in $\mathrm{PSL}_4(3)$, $G/(G \cap Z)$ should contain an element of order $\frac{3^4-1}{2(3-1)} = 20$. In the Atlas of Finite Groups [1], there is a complete list of the conjugacy classes of maximal subgroups of $\mathrm{PSL}_4(3)$, from which list only four conjugacy classes consist of subgroups with orders divisible by 20. One of them is the class of extension field type subgroups, there is one class of maximal subgroups isomorphic to S_6 and there are two conjugacy classes of maximal subgroups with structure $\mathrm{PSp}_4(3) : 2$. However, S_6 has no elements of order 20 and $\mathrm{PSp}_4(3)$ has no elements of order 10. Therefore, G must be an extension field type subgroup.

If $p^{fd} - 1$ does not have a primitive prime divisor, then $p^{fd} = 64$, and since the $(d,q) = (3,4)$ case is already excluded, we may assume that $p = q = 2$ and $d = 6$. Then $\mathrm{SL}_d(q) = \mathrm{SL}_6(2) = \mathrm{GL}_6(2)$ and by W. M. Kantor [6], all the maximal overgroups of the Singer elements of $\mathrm{GL}_6(2)$ are extension field type subgroups. ■

Theorem 2.3.5 *Suppose $G \leq Sp_d(q)$ is a maximal overgroup of a Singer cycle of $Sp_d(q)$, $d \geq 4$, $q = p^f$ is an odd prime power and $(d,q) \neq (4,3)$. Then G is an extension field type subgroup of $Sp_d(q)$, isomorphic to either $GU_{\frac{d}{2}}(q^2).2$ or $Sp_{\frac{d}{r}}(q^r) \cdot r$ for some prime divisor r of d.*

Proof: We may assume that $p^{fd} - 1$ has a primitive prime divisor, since p is odd and $d \geq 4$. Therefore, $G \in \mathcal{S}(d,q)$. As in the proof of the previous theorem, it is easy to see (except for the case $(d,q) = (6,3)$) that $G \notin \mathcal{S}_1(d,q) \cup \mathcal{S}_3(d,q) \cup \mathcal{S}_4(d,q)$. This means that G must be inside an extension field type subgroup of $\mathrm{GL}_d(q)$

corresponding to a prime divisor r of d. Now suppose $(d, q) = (6, 3)$. Then the image of G in $\mathrm{PSp}_6(3)$, $G/(G \cap Z)$ should contain an element of order $\frac{1}{2}(3^3 + 1) = 14$. In the Atlas of Finite Groups [1], there is a complete list of the conjugacy classes of maximal subgroups of $\mathrm{PSp}_6(3)$, from which list only three conjugacy classes consist of subgroups with orders divisible by 14. Two of them are the extension field type subgroups corresponding to the two prime divisors of 6, and there is one conjugacy class of maximal subgroups isomorphic to $\mathrm{PSL}_2(13)$. However, $\mathrm{PSL}_2(13)$ does not have elements of order 14, therefore G must be an extension field type subgroup of $\mathrm{Sp}_6(3)$. ■

Theorem 2.3.6 *Let G be a maximal subgroup of $SL_2(q) = Sp_2(q)$ containing an element of order $q+1$ ($q = p^f$, p a prime number), and assume that $q \notin \{2, 5, 7, 9\}$. Then G is an extension field type subgroup in $SL_2(q)$.*

Proof: If $q = 3$ then the singer elements of $\mathrm{SL}_2(q) = \mathrm{SL}_2(3)$ are of order 4 and their only maximal overgroup is the unique Sylow 2-subgroup of $\mathrm{SL}_2(3)$, which is actually an extension field type subgroup of $\mathrm{SL}_2(3) = \mathrm{Sp}_2(3)$.

From now we assume that $q \geq 4$. Let Z denote the center of $\mathrm{GL}_2(q)$. Since G contains an element of order $q+1$, the image of G in $\mathrm{PSL}_2(q)$, $G/(G \cap Z)$ must contain an element of order $\frac{1}{\gcd(q+1,2)}(q+1)$. It is known that $G/(G \cap Z)$ as a maximal subgroup of $\mathrm{PSL}_2(q)$, has to be isomorphic to either a dihedral group of order $\frac{2(q\pm1)}{\gcd(q-1,2)}$, or A_4, S_4, A_5, $\mathrm{PSL}_2(p^e)$ or $\mathrm{PGL}_2(p^e)$ for some divisor e of f with $e < f$. (Further details about the classification of maximal subgroups of $\mathrm{PSL}_2(q)$ can be found for example in the first volume of M. Suzuki's well-known book on Group Theory [13].) From Lemma 2.3.2 we know that the largest element order in $\mathrm{PSL}_2(p^e)$ is $p^e + 1$, which is always less then $\frac{1}{\gcd(q+1,2)}(q+1)$. Hence $G/(G \cap Z)$ cannot be isomorphic to $\mathrm{PSL}_2(p^e)$ or $\mathrm{PGL}_2(p^e)$.

Next assume that $G/(G \cap Z) \simeq A_5$. Then $q(q^2 - 1) \equiv 0 \pmod 5$, otherwise $\mathrm{PSL}_2(q)$ would not contain a subgroup isomorphic to A_5. And since the largest element order in A_5 is 5, we must have $\frac{1}{\gcd(q+1,2)}(q+1) \leq 5$. This implies $q = 4$, 5 or 9, but for $q \in \{4,5\}$, $\mathrm{PSL}_2(q) \simeq A_5$, so G would not be a proper subgroup of $\mathrm{SL}_2(q)$. For $q = 9$, $\mathrm{PSL}_2(q) \simeq A_6$ does have a maximal subgroup isomorphic to A_5.

Now assume that $G/(G \cap Z) \simeq S_4$. Then $q^2 \equiv 1 \pmod{16}$ is a necessary condition for q, and the largest element order in S_4 is 4, so we must have $\frac{1}{\gcd(q+1,2)}(q+1) \leq 4$. This implies $q = 7$. If $G/(G \cap Z) \simeq A_4$, then $\frac{1}{\gcd(q+1,2)}(q+1) \leq 3$ and $q = 5$.

Finally, $G/(G \cap Z)$ cannot be isomorphic to the dihedral group of order $\frac{2(q-1)}{\gcd(q-1,2)}$, so if $q \notin \{2,5,7,9\}$ then $G/(G \cap Z)$ is isomorphic to the dihedral group of order $\frac{2(q+1)}{\gcd(q-1,2)}$, in which case G is an extension field type subgroup in $\mathrm{SL}_2(q) = \mathrm{SP}_2(q)$.

■

Remarks: In $\mathrm{SL}_2(5)$, there are two conjugacy classes of maximal subgroups containing Singer elements, that is, elements of order 6. One class has subgroups of index 5, isomorphic to $\mathrm{SL}_2(3)$ and the other class has subgroups of index 10, isomorphic to the group defined by the presentation $\langle x, y \mid x^6 = 1, x^3 = y^2, y^{-1}xy = x^{-1} \rangle$.

In $\mathrm{SL}_2(7)$, every maximal subgroup containing an element of order 8 is a central extension of S_4 by Z_2, and there are two conjugacy classes of them.

In $\mathrm{SL}_2(9)$, every maximal subgroup containing an element of order 10 is isomorphic to $\mathrm{SL}_2(5)$, and there are two conjugacy classes of these subgroups.

In $\mathrm{SL}_3(4)$, there are three conjugacy classes of maximal subgroups containing elements of order 21. These are all conjugate in $\mathrm{GL}_3(4)$ and they have a structure of $\mathrm{SL}_3(2).3$.

In $\mathrm{Sp}_4(3)$, beside the extension field type subgroups (isomorphic to $Z_2 \ltimes \mathrm{Sp}_2(9)$), there is another conjugacy class of maximal subgroups that contain elements of order $3^2 + 1 = 10$. This conjugacy class consists of subgroups of index 27, with their image in $\mathrm{PSp}_4(3)$ isomorphic to $\mathrm{SL}_2(4) \ltimes (\mathbf{F}_4 \oplus \mathbf{F}_4)$.

CHAPTER 3
CENTRALIZER ORDERS

3.1 Elements of Order p with Homogeneous Action in GL Groups

In this section V is a vector space of dimension d over $\mathbf{F}_q$ ($q = p^f$) and g is an element of $\mathrm{GL}(V)$ with $g^p = 1$, acting homogeneously on V. By homogeneous action we mean that V decomposes into a direct sum of isomorphic indecomposable $\mathbf{F}_q\langle g\rangle$-modules, say $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$ where each V_i is an indecomposable $\mathbf{F}_q\langle g\rangle$-module of dimension a. Then of course, $a \leq p$ and $ab = d$.

Since $g^p = 1$, $x = g - 1$ is a nilpotent endomorphism of V with $x^p = 0$. And because V consists of only $\mathbf{F}_q\langle g\rangle$-modules of dimension a, it is also true that $x^a = 0$. Let W be the kernel of x, so W is a b-dimensional subspace of V that is determined by g.

Definition 3.1.1 *Let $\{v_1, v_2, \ldots, v_b\}$ be a subset of V such that $\beta = \{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$ is a basis for V. Then we say that β together with the ordering of the set $\{v_1, v_2, \ldots, v_b\}$ is a* **standard basis** *for (V, g).*

Lemma 3.1.2 *The number of standard bases for (V, g) is*

$$q^{(a-1)b^2} \cdot |GL(W)| = q^{ab^2} \cdot \prod_{k=1}^{b} \left(1 - \frac{1}{q^k}\right).$$

Proof: Notice that if $\{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$ is a standard basis for (V, g) then the set $\{v_i x^{a-1} \mid 1 \leq i \leq b\}$ must be a basis for W. Now let $\overline{\beta} = \{w_1, w_2, \ldots, w_b\}$ be any ordered basis for W. Then for each integer $1 \leq i \leq b$ there are exactly $q^{(a-1)b}$ vectors v_i with the property that $v_i x^{a-1} = w_i$. And if $\{v_1, v_2, \ldots v_b\}$ is any ordered set such that $v_i x^{a-1} = w_i$ for all i then $\beta = \{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$ is a standard basis for (V,g). This shows that for any given ordered basis $\overline{\beta}=\{w_1,w_2,\ldots,w_b\}$ for W the number of standard bases $\beta=\{v_ix^k\,|\,1\le i\le b, 0\le k\le a-1\}$ for (V,g) with $v_ix^{a-1}=w_i$ $(1\le i\le b)$ is equal to $q^{(a-1)b^2}$. And since the number of ordered bases for W is the same as the order of $\mathrm{GL}(W)$, the number of standard bases for (V,g) is $q^{(a-1)b^2}\cdot|\mathrm{GL}(W)|$. ■

Theorem 3.1.3

$$|C_{\mathrm{GL}(V)}(g)|=q^{ab^2}\cdot\prod_{k=1}^{b}\left(1-\frac{1}{q^k}\right).$$

Proof: It is enough to show that $C_{\mathrm{GL}(V)}(g)$ acts transitively on the set of standard bases for (V,g). So let $\beta_1=\{v_ix^k\,|\,1\le i\le b, 0\le k\le a-1\}$ and $\beta_2=\{u_ix^k\,|\,1\le i\le b, 0\le k\le a-1\}$ be standard bases for (V,g). Define the linear transformation $z\in\mathrm{GL}(V)$ as follows:

$$\begin{aligned} z:V &\longrightarrow V\\ v_ix^k &\longmapsto u_ix^k \quad (1\le i\le b, 0\le k\le a-1)\,. \end{aligned}$$

Then clearly $\beta_1 z=\beta_2$ and $z\in C_{\mathrm{GL}(V)}(g)$. ■

3.2 Elements of Order p with Homogeneous Action in Sp Groups

In this section, V is a vector space of dimension d over $\mathbf{F}_q$ ($q=p^f$ an odd prime power) equipped with a non-singular symplectic form B, $I(V,B)$ is the isometry group of (B,V), and g is an element of $I(V,B)$ with $g^p=1$, acting homogeneously on V. By the homogeneous action of g we mean that V decomposes into a direct sum of isomorphic indecomposable $\mathbf{F}_q\langle g\rangle$-modules, say $V=V_1\oplus V_2\oplus\ldots\oplus V_b$ where each V_i is an indecomposable $\mathbf{F}_q\langle g\rangle$-module of dimension a. Then of course, $a\le p$ and $ab=d$. Also, let δ be a fixed quadratic non-residue in $\mathbf{F}_q$.

As before, τ is the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_q}(V)$ with the property that

$$B(u\phi,v)=B(u,v\tau(\phi))$$

for all u, v in V and ϕ in $\mathrm{End}_{\mathbf{F}_q}(V)$. Since $g^p = 1$, $x = g - 1$ is a nilpotent endomorphism of V with $x^p = 0$. And because V consists of only $\mathbf{F}_q\langle g\rangle$-modules of dimension a, it is also true that $x^a = 0$. Let W be the kernel of x, which is also the image of V under x^{a-1}, so W is a b-dimensional subspace of V that is determined by g.

Notice that $1 = g\tau(g) = (1+x)(1+\tau(x)) = 1 + x + \tau(x) + x\tau(x)$, hence

$$x + \tau(x) + x\tau(x) = 0\,,$$

$$\begin{aligned}\tau(x) &= -x(1+x)^{-1}\\ &= \sum_{k=1}^{a-1}(-1)^k x^k\,.\end{aligned}$$

In the following two lemmas we will prove two elementary properties of x, which properties are also true if B is a non-singular symmetric or unitary form instead of being a symplectic form.

Lemma 3.2.1 *If $k + l \geq a$ then $B(ux^k, vx^l) = 0$ for any $u, v \in V$. If $k + l = a - 1$ then $B(ux^k, vx^l) = (-1)^k B(u, vx^{a-1})$ for any $u, v \in V$. In particular $B(ux^{a-1}, v) = (-1)^{a-1}B(u, vx^{a-1})$ for all $u, v \in V$.*

Proof: $B(ux^k, vx^l) = B(u, vx^l\tau(x)^k)$ for any $u, v \in V$ and

$$\begin{aligned}x^l\tau(x)^k &= x^l(-x - x\tau(x))^k\\ &= (-1)^k x^{l+k}(1+\tau(x))^k\,.\end{aligned}$$

So if $k + l \geq a$ then $x^{k+l} = 0$ and hence $x^l\tau(x)^k = 0$, and if $k + l = a - 1$ then $x^l\tau(x)^k = (-1)^k x^{a-1}(1+\tau(x))^k = (-1)^k x^{a-1}(1 - x - x\tau(x))^k = (-1)^k x^{a-1}$. ■

Lemma 3.2.2 *For any non-negative integer l there is a polynomial $h_l(t)$ of degree $2l + 1$ with integer coefficients such that for any $u, v \in V$*

$$B(u, vx^{2l}) = (-1)^l B(ux^l, vx^l) + B(u, v\, h_l(x))\,.$$

Proof: Since $x + \tau(x) + x\tau(x) = 0$, $x = -\tau(x)(1 + x)$ and

$$\begin{aligned} x^{2l} &= x^l(-\tau(x)(1+x))^l \\ &= (-1)^l x^l \tau(x)^l (1+x)^l \\ &= (-1)^l x^l \tau(x)^l + (-1)^l x^l \tau(x)^l (\sum_{i=1}^{l} \binom{l}{i} x^i) \\ &= (-1)^l x^l \tau(x)^l + h_l(x) \end{aligned}$$

where $h_l(t) = (-1)^l t^l (\sum_{i=1}^{a-1} (-1)^i t^i)^l (\sum_{i=1}^{l} \binom{l}{i} t^i) = t^l (\sum_{i=1}^{a-1} (-1)^{i-1} t^i)^l (\sum_{i=1}^{l} \binom{l}{i} t^i)$. Hence for any $u, v \in V$

$$\begin{aligned} B(u, vx^{2l}) &= B(u, v[(-1)^l x^l \tau(x)^l + h_l(x)]) \\ &= (-1)^l B(ux^l, vx^l) + B(u, vh_l(x)) \ . \quad \blacksquare \end{aligned}$$

In this section, we will show that g defines a non-singular bilinear form $\overline{B}$ in a natural way on W, which is either symmetric or symplectic. Then we will show that this bilinear form characterizes the conjugacy class of g in $I(V, B)$, and finally we will give a formula for the order of the centralizer of g in $I(V, B)$.

Definition 3.2.3 *Define $\overline{B}$ as follows:*

$$\overline{B} : W \times W \rightarrow \mathbf{F}_q$$

$$\overline{B}(ux^{a-1}, vx^{a-1}) = B(u, vx^{a-1})$$

Lemma 3.2.4 *$\overline{B}$ is a well-defined non-singular bilinear form on W. Furthermore, if a is even then $\overline{B}$ is symmetric, and if a is odd then $\overline{B}$ is symplectic.*

Proof: If $u_1x^{a-1} = ux^{a-1}$ and $v_1x^{a-1} = vx^{a-1}$ then

$$\begin{aligned} B(u_1, v_1x^{a-1}) &= B(u + (u_1 - u), vx^{a-1}) \\ &= B(u, vx^{a-1}) + B(u_1 - u, vx^{a-1}) \\ &= B(u, vx^{a-1}) + (-1)^{a-1}B((u_1 - u)x^{a-1}, v) \\ &= B(u, vx^{a-1}) + (-1)^{a-1}B(0, v) \\ &= B(u, vx^{a-1})\,. \end{aligned}$$

This shows that $\overline{B}$ is well-defined. To prove the other statement of the lemma:

$$\begin{aligned} \overline{B}(ux^{a-1}, vx^{a-1}) &= B(u, vx^{a-1}) \\ &= -B(vx^{a-1}, u) \\ &= -(-1)^{a-1}B(v, ux^{a-1}) \\ &= (-1)^{a}\overline{B}(vx^{a-1}, ux^{a-1})\,. \end{aligned}$$

Hence $\overline{B}$ is symmetric if a is even, and symplectic if a is odd. Finally, the non-singularity of $\overline{B}$ follows obviously from the non-singularity of B. ∎

Lemma 3.2.5 *If $\varphi \in I(V, B)$ commutes with g then for any $u, v \in W$, $\overline{B}(u\varphi, v\varphi) = \overline{B}(u, v)$.*

Proof: Notice that the fact that φ is a non-singular transformation that commutes with g, already implies that $W\varphi = W$. And if $u = u_1x^{a-1}$, $v = v_1x^{a-1}$ then $u\varphi = u_1\varphi x^{a-1}$ and

$$\overline{B}(u\varphi, v\varphi) = B(u_1\varphi, v_1x^{a-1}\varphi) = B(u_1, v_1x^{a-1}) = \overline{B}(u, v)\,. \quad ∎$$

Definition 3.2.6 *Let $\overline{\beta} = \{w_1, w_2, \ldots, w_b\}$ be an ordered basis for W. We say that $\overline{\beta}$ is a* **standard basis** *for $(W, \overline{B})$ if one of the following holds:*

1. *$\overline{B}$ is symmetric and*

$$\overline{B}(v_i, v_j) = \begin{cases} 0, & \text{if } i \neq j \ ; \\ 1, & \text{if } i = j \leq b-1 \ ; \\ 1 \text{ or } \delta, & \text{if } i = j = b \ . \end{cases}$$

2. *$\overline{B}$ is symplectic and*

$$\overline{B}(v_i, v_j) = \begin{cases} 0, & \text{if } i+j \neq b+1 \ ; \\ 1, & \text{if } i > j \text{ and } i+j = b+1 \ ; \\ -1, & \text{if } i < j \text{ and } i+j = b+1 \ . \end{cases}$$

Definition 3.2.7 *Let $\{v_1, v_2, \ldots, v_b\}$ be an ordered subset of V such that*

$$\beta = \{ \, v_i x^k \mid 1 \leq i \leq b \, , \, 0 \leq k \leq a-1 \, \}$$

is a basis for V. We say that β together with the ordering of $\{v_1, v_2, \ldots, v_b\}$ is a **standard basis** *for (V, B, g) if*

1. *$\{v_i x^{a-1} \mid 1 \leq i \leq b\}$ is a standard basis for $(W, \overline{B})$*

2. *$B(v_i, v_j x^k) = 0$ whenever $k < a-1$ and either $i < j$ or $i = j$ and k is odd.*

We will prove the existence of a standard basis for (V, B, g), but in order to do that first we need to prove some technical lemmas.

Lemma 3.2.8 *Suppose that a is even, so $\overline{B}$ is symmetric on W and let $w \in W$ be any nonzero vector. Define $\mathcal{S}_w$ to be the set of all vectors $v \in V$ such that $vx^{a-1} = w$ and $B(v, vx^k) = 0$ for every odd number k between 0 and $a-2$. Then*

$$|\mathcal{S}_w| = q^{(a-1)b - \frac{a}{2} + 1} \ .$$

Proof: If $a = 2$ then $q^{(a-1)b-\frac{a}{2}+1} = q^b$, and $\mathcal{S}_w$ is simply the set $\{v \in V | vx = w\}$ so $|\mathcal{S}_w| = |\ker(x)| = q^b$ also. Hence from now on, we may assume that $a \geq 4$. Let

$$W_1 = \{v \in V \mid vx^{a-1} = w\}$$

and define the maps φ_i $(1 \le i \le \frac{a}{2} - 1)$ and sets W_i $(2 \le i \le \frac{a}{2})$ as follows. For any $1 \le i \le \frac{a}{2} - 1$ let

$$\begin{aligned} \varphi_i : W_i &\longrightarrow \mathbf{F}_q \\ v &\longmapsto B(v, vx^{a-2i-1}) \\ W_{i+1} &= \{v \in W_i \mid \varphi_i(v) = 0\} . \end{aligned}$$

Since $\mathcal{S}_w = W_{\frac{a}{2}}$ and $|W_1| = q^{(a-1)b}$, it will be enough to show that $|W_i| = \frac{1}{q}|W_{i-1}|$ for all $2 \le i \le \frac{a}{2}$.

First let v be any vector in W_1. Then for any $v' \in V$, $v + v'x^2$ is also in W_1 and

$$\begin{aligned} \varphi_1(v + v'x^2) &= B(v + v'x^2, (v + v'x^2)x^{a-3}) \\ &= B(v, vx^{a-3}) + B(v, v'x^{a-1}) + B(v'x^2, vx^{a-3}) \\ &= B(v, vx^{a-3}) + B(v, v'x^{a-1}) + B(v', vx^{a-1}) \\ &= B(v, vx^{a-3}) + 2B(v, v'x^{a-1}) \\ &= \varphi_1(v) + 2\overline{B}(vx^{a-1}, v'x^{a-1}) \\ &= \varphi_1(v) + 2\overline{B}(w, v'x^{a-1}) . \end{aligned}$$

Notice that the map

$$Vx^2 \longrightarrow \mathbf{F}_q$$

$$v'x^2 \longmapsto 2\overline{B}(w, v'x^{a-1})$$

is a well-defined non-trivial linear map, so

$$|W_2 \cap \{v + Vx^2\}| = \frac{1}{q}|\{v + Vx^2\}| .$$

This is true for any $v \in W_1$, therefore

$$|W_2| = \frac{1}{q}|W_1 + Vx^2| = \frac{1}{q}|W_1| .$$

Now assume that $2 \leq l \leq \frac{a}{2} - 1$ and $|W_i| = \frac{1}{q}|W_{i-1}|$ for all $i \leq l$. In particular, this means that W_l is a non-empty set. We want to show that $|W_{l+1}| = \frac{1}{q}|W_l|$. In order to do this, first choose an element v from W_l. Then for any $v' \in V$, $v + v'x^{2l}$ is also en element of W_l, because $v + v'x^{2l} \in W_1$ and for any $0 \leq i \leq l-1$, $a - 2i + 2l - 1 \geq a + 1$ and hence

$$\begin{aligned} \varphi_i(v + v'x^{2l}) &= B(v + v'x^{2l}, (v + v'x^{2l})x^{a-2i-1}) \\ &= B(v, vx^{a-2i-1}) \\ &= \varphi_i(v) = 0 \,. \end{aligned}$$

Furthermore,

$$\begin{aligned} \varphi_l(v + v'x^{2l}) &= B(v + v'x^{2l}, (v + v'x^{2l})x^{a-2l-1}) \\ &= B(v, vx^{a-2l-1}) + B(v, v'x^{a-1}) + B(v'x^{2l}, vx^{a-2l-1}) \\ &= B(v, vx^{a-2l-1}) + B(v, v'x^{a-1}) + B(v', vx^{a-1}) \\ &= \varphi_l(v) + 2\overline{B}(vx^{a-1}, v'x^{a-1}) \\ &= \varphi_l(v) + 2\overline{B}(w, v'x^{a-1}) \,. \end{aligned}$$

Again, the map

$$\begin{aligned} Vx^{2l} &\longrightarrow \mathbf{F}_q \\ v'x^{2l} &\longmapsto 2\overline{B}(w, v'x^{a-1}) \end{aligned}$$

is a well-defined non-trivial linear map, so

$$|W_{l+1} \cap \{v + Vx^{2l}\}| = \frac{1}{q}|\{v + Vx^{2l}\}| \,.$$

This is true for any $v \in W_l$, therefore

$$|W_{l+1}| = \frac{1}{q}|W_l + Vx^{2l}| = \frac{1}{q}|W_l| \,.$$

This completes the proof of this lemma. ■

Lemma 3.2.9 *Suppose that a is an odd number, so $\overline{B}$ is a symplectic form on W and let $(w_1, w_2) \in W \times W$ be a pair of linearly independent vectors. Define $\mathcal{S}_{w_1,w_2}$ to be the set of all pairs $(v_1, v_2) \in V \times V$ such that $v_1 x^{a-1} = w_1$, $v_2 x^{a-1} = w_2$, $B(v_1, v_2 x^k) = 0$ for all $0 \leq k \leq a-2$ and $B(v_1, v_1 x^k) = B(v_2, v_2 x^k) = 0$ for any odd number k between 0 and $a-1$. Then*

$$|\mathcal{S}_{w_1,w_2}| = q^{2(a-1)(b-1)} .$$

Proof: If $a = 1$ then $\mathcal{S}_{w_1,w_2} = \{(w_1, w_2)\}$ and there is nothing really to prove. So from now on, we may assume that $a \geq 3$. Let

$$W_1 = \{(v_1, v_2) \in V \times V \,|\, (v_1 x^{a-1}, v_2 x^{a-1}) = (w_1, w_2)\} ,$$

and define the maps φ_i for $1 \leq i \leq a-1$ and sets W_i for $2 \leq i \leq a$ as follows. For any $1 \leq i \leq \frac{a-1}{2}$ let

$$\begin{aligned} \varphi_{2i-1} : W_{2i-1} &\longrightarrow \mathbf{F}_q^{\,3} \\ (v_1, v_2) &\longmapsto (\,B(v_1, v_1 x^{a-2i}), B(v_1, v_2 x^{a-2i}), B(v_2, v_2 x^{a-2i})\,) \end{aligned}$$

$$W_{2i} = \{(v_1, v_2) \in W_{2i-1} \,|\, \varphi_{2i-1}(v_1, v_2) = (0,0,0)\}$$

$$\begin{aligned} \varphi_{2i} : W_{2i} &\longrightarrow \mathbf{F}_q \\ (v_1, v_2) &\longmapsto B(v_1, v_2 x^{a-2i-1}) \end{aligned}$$

$$W_{2i+1} = \{(v_1, v_2) \in W_{2i} \,|\, \varphi_{2i}(v_1, v_2) = 0\} .$$

Since $\mathcal{S}_{w_1,w_2} = W_a$ and $|W_1| = q^{2(a-1)b}$, it will be enough to show that $|W_{2i}| = \frac{1}{q^3}|W_{2i-1}|$ and $|W_{2i+1}| = \frac{1}{q}|W_{2i}|$ for all $1 \leq i \leq \frac{a-1}{2}$.

First let (v_1, v_2) be any pair in W_1. Then for any (v_1', v_2') in $V \times V$, $(v_1 + v_1' x, v_2 + v_2' x)$ is also an element of W_1 and

$$\begin{aligned} \varphi_1(v_1 + v_1' x, v_2 + v_2' x) \;=\; (\,& B(v_1 + v_1' x, (v_1 + v_1' x) x^{a-2}), \\ & B(v_1 + v_1' x, (v_2 + v_2' x) x^{a-2}), \\ & B(v_2 + v_2' x, (v_2 + v_2' x) x^{a-2})\,) \end{aligned}$$

$$\begin{aligned}
&= (\,B(v_1, v_1x^{a-2}) + B(v_1, v_1'x^{a-1}) + B(v_1'x, v_1x^{a-2}),\\
&\qquad B(v_1, v_2x^{a-2}) + B(v_1, v_2'x^{a-1}) + B(v_1'x, v_2x^{a-2}),\\
&\qquad B(v_2, v_2x^{a-2}) + B(v_2, v_2'x^{a-1}) + B(v_2'x, v_2x^{a-2})\,)\\
&= (\,B(v_1, v_1x^{a-2}) + B(v_1, v_1'x^{a-1}) - B(v_1', v_1x^{a-1}),\\
&\qquad B(v_1, v_2x^{a-2}) + B(v_1, v_2'x^{a-1}) - B(v_1', v_2x^{a-1}),\\
&\qquad B(v_2, v_2x^{a-2}) + B(v_2, v_2'x^{a-1}) - B(v_2', v_2x^{a-1})\,)\\
&= (\,B(v_1, v_1x^{a-2}) + 2\overline{B}(v_1x^{a-1}, v_1'x^{a-1}),\\
&\qquad B(v_1, v_2x^{a-2}) + 2\overline{B}(v_1x^{a-1}, v_2'x^{a-1}),\\
&\qquad B(v_2, v_2x^{a-2}) + 2\overline{B}(v_2x^{a-1}, v_2'x^{a-1})\,)\\
&= \varphi_1(v_1, v_2) +\\
&\qquad +2(\,\overline{B}(w_1, v_1'x^{a-1}), \overline{B}(w_1, v_2'x^{a-1}), \overline{B}(w_2, v_2'x^{a-1})\,)\,.
\end{aligned}$$

Notice that the map

$$\begin{aligned}
Vx \oplus Vx &\longrightarrow \mathbf{F}_q{}^3\\
(v_1'x, v_2'x) &\longmapsto
\end{aligned}$$

$$\longmapsto 2(\,\overline{B}(w_1, v_1'x^{a-1}), \overline{B}(w_1, v_2'x^{a-1}), \overline{B}(w_2, v_2'x^{a-1})\,)$$

is a well-defined linear map, and it is onto, hence it follows that

$$|W_2 \cap \{(v_1, v_2) + (Vx, Vx)\}| = \frac{1}{q^3}|\{(v_1, v_2) + (Vx, Vx)\}|\,.$$

This is true for any (v_1, v_2) in W_1, therefore

$$|W_2| = \frac{1}{q^3}|\{W_1 + (Vx, Vx)\}| = \frac{1}{q^3}|W_1|\,.$$

Next, let $(v_1, v_2) \in W_2$. Then for any v_1' in V, $(v_1 + v_1'x^2, v_2)$ is also in W_2 since it is in W_1 and

$$\begin{aligned}
\varphi_1(v_1 + v_1'x^2, v_2) &= (\, B(v_1 + v_1'x^2, (v_1 + v_1'x^2)x^{a-2}), \\
&\qquad B(v_1 + v_1'x^2, v_2x^{a-2}), B(v_2, v_2x^{a-2})\,) \\
&= (\, B(v_1, v_1x^{a-2}), B(v_1, v_2x^{a-2}), B(v_2, v_2x^{a-2})\,) \\
&= \varphi_1(v_1, v_2) = 0\ .
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\varphi_2(v_1 + v_1'x^2, v_2) &= B(v_1 + v_1'x^2, v_2x^{a-3}) \\
&= B(v_1, v_2x^{a-3}) + B(v_1'x^2, v_2x^{a-3}) \\
&= B(v_1, v_2x^{a-3}) + B(v_1', v_2x^{a-1}) \\
&= \varphi_2(v_1, v_2) + \overline{B}(v_1'x^{a-1}, v_2x^{a-1}) \\
&= \varphi_2(v_1, v_2) + \overline{B}(v_1'x^{a-1}, w_2)\ .
\end{aligned}$$

Again, the map

$$\begin{aligned}
Vx^2 &\longrightarrow \mathbf{F}_q \\
v_1'x^2 &\longmapsto \overline{B}(v_1'x^{a-1}, w_2)
\end{aligned}$$

is a well-defined non-trivial linear map, so it follows that

$$|W_3 \cap \{(v_1 + Vx^2, v_2)\}| = \frac{1}{q}|\{(v_1 + Vx^2, v_2)\}|\ .$$

This is true for any $(v_1, v_2) \in W_2$, therefore

$$|W_3| = \frac{1}{q}|W_2|\ .$$

Now assume that $2 \leq l \leq \frac{a-1}{2}$ and $|W_{2i}| = \frac{1}{q^3}|W_{2i-1}|$ and $|W_{2i+1}| = \frac{1}{q}|W_{2i}|$ for all $1 \leq i < l$. In particular, this means that W_{2l-1} is a non-empty set. We want to show that $|W_{2l}| = \frac{1}{q^3}|W_{2l-1}|$ and $|W_{2l+1}| = \frac{1}{q}|W_{2l}|$. In order to do this, first choose a pair (v_1, v_2) from W_{2l-1}. Than for any $(v_1', v_2') \in V \times V$, $(v_1 + v_1' x^{2l-1}, v_2 + v_2' x^{2l-1})$ is also in W_{2l-1} since it is in W_1 and for any $1 \leq j < 2l$ it is true that

$$\begin{aligned} B(v_1 + v_1' x^{2l-1}, (v_1 + v_1' x^{2l-1}) x^{a-j}) &= B(v_1, v_1 x^{a-j}), \\ B(v_1 + v_1' x^{2l-1}, (v_2 + v_2' x^{2l-1}) x^{a-j}) &= B(v_1, v_2 x^{a-j}), \\ B(v_2 + v_2' x^{2l-1}, (v_2 + v_2' x^{2l-1}) x^{a-j}) &= B(v_2, v_2 x^{a-j}). \end{aligned}$$

Furthermore,

$$\begin{aligned} \varphi_{2l-1}(v_1 + v_1' x^{2l-1}, v_2 + v_2' x^{2l-1}) &= (\, B(v_1 + v_1' x^{2l-1}, (v_1 + v_1' x^{2l-1}) x^{a-2l}), \\ &\qquad B(v_1 + v_1' x^{2l-1}, (v_2 + v_2' x^{2l-1}) x^{a-2l}), \\ &\qquad B(v_2 + v_2' x^{2l-1}, (v_2 + v_2' x^{2l-1}) x^{a-2l})\,) \\ &= (\, B(v_1, v_1 x^{a-2l}) + B(v_1, v_1' x^{a-1}) + B(v_1' x^{2l-1}, v_1 x^{a-2l}), \\ &\qquad B(v_1, v_2 x^{a-2l}) + B(v_1, v_2' x^{a-1}) + B(v_1' x^{2l-1}, v_2 x^{a-2l}), \\ &\qquad B(v_2, v_2 x^{a-2l}) + B(v_2, v_2' x^{a-1}) + B(v_2' x^{2l-1}, v_2 x^{a-2l})\,) \\ &= (\, B(v_1, v_1 x^{a-2l}) + B(v_1, v_1' x^{a-1}) - B(v_1', v_1 x^{a-1}), \\ &\qquad B(v_1, v_2 x^{a-2l}) + B(v_1, v_2' x^{a-1}) - B(v_1', v_2 x^{a-1}), \\ &\qquad B(v_2, v_2 x^{a-2l}) + B(v_2, v_2' x^{a-1}) - B(v_2', v_2 x^{a-1})\,) \\ &= (\, B(v_1, v_1 x^{a-2}) + 2\overline{B}(v_1 x^{a-1}, v_1' x^{a-1}), \\ &\qquad B(v_1, v_2 x^{a-2}) + 2\overline{B}(v_1 x^{a-1}, v_2' x^{a-1}), \\ &\qquad B(v_2, v_2 x^{a-2}) + 2\overline{B}(v_2 x^{a-1}, v_2' x^{a-1})\,) \\ &= \varphi_{2l-1}(v_1, v_2) + \\ &\qquad +2(\, \overline{B}(w_1, v_1' x^{a-1}), \overline{B}(w_1, v_2' x^{a-1}), \overline{B}(w_2, v_2' x^{a-1})\,). \end{aligned}$$

Notice that the map

$$\begin{aligned} V x^{2l-1} \oplus V x^{2l-1} &\longrightarrow \mathbf{F}_q{}^3 \\ (v_1' x^{2l-1}, v_2' x^{2l-1}) &\longmapsto 2(\, \overline{B}(w_1, v_1' x^{a-1}), \overline{B}(w_1, v_2' x^{a-1}), \overline{B}(w_2, v_2' x^{a-1})\,) \end{aligned}$$

is a well-defined linear map, and it is onto, hence it follows that

$$|W_{2l} \cap \{(v_1, v_2) + (Vx^{2l-1}, Vx^{2l-1})\}| = \frac{1}{q^3} |\{(v_1, v_2) + (Vx^{2l-1}, Vx^{2l-1})\}| \, .$$

This is true for any (v_1, v_2) in W_{2l-1}, therefore

$$|W_{2l}| = \frac{1}{q^3} |\{W_{2l-1} + (Vx, Vx)\}| = \frac{1}{q^3} |W_{2l-1}| \, .$$

Next, let $(v_1, v_2) \in W_{2l}$. Then for any v_1' in V, $(v_1 + v_1' x^{2l}, v_2)$ is also in W_{2l} since it is in W_1 and for any $1 \leq j \leq 2l$ it is true that

$$\begin{aligned}
B(v_1 + v_1' x^{2l}, (v_1 + v_1' x^{2l}) x^{a-j}) &= B(v_1, v_1 x^{a-j}) \, , \\
B(v_1 + v_1' x^{2l}, (v_2 + v_2' x^{2l}) x^{a-j}) &= B(v_1, v_2 x^{a-j}) \, , \\
B(v_2 + v_2' x^{2l}, (v_2 + v_2' x^{2l}) x^{a-j}) &= B(v_2, v_2 x^{a-j}) \, .
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\varphi_{2l}(v_1 + v_1' x^{2l}, v_2) &= B(v_1 + v_1' x^{2l}, v_2 x^{a-2l-1}) \\
&= B(v_1, v_2 x^{a-2l-1}) + B(v_1' x^{2l}, v_2 x^{a-2l-1}) \\
&= B(v_1, v_2 x^{a-2l-1}) + B(v_1', v_2 x^{a-1}) \\
&= \varphi_{2l}(v_1, v_2) + \overline{B}(v_1' x^{a-1}, v_2 x^{a-1}) \\
&= \varphi_{2l}(v_1, v_2) + \overline{B}(v_1' x^{a-1}, w_2) \, .
\end{aligned}$$

Again, the map

$$\begin{aligned}
Vx^{2l} &\longrightarrow \mathbf{F}_q \\
v_1' x^{2l} &\longmapsto \overline{B}(v_1' x^{a-1}, w_2)
\end{aligned}$$

is a well-defined non-trivial linear map, so it follows that

$$|W_{2l+1} \cap \{(v_1 + Vx^{2l}, v_2)\}| = \frac{1}{q} |\{(v_1 + Vx^{2l}, v_2)\}| \, .$$

This is true for any $(v_1, v_2) \in W_{2l}$, therefore

$$|W_{2l+1}| = \frac{1}{q}|W_{2l}| .$$

This completes the proof of the lemma. ■

Lemma 3.2.10 *Suppose that a is even. Then the number of standard bases for (V, B, g) is*

$$q^{\frac{(a-1)b^2+b}{2}} \cdot |I(W, \overline{B})| .$$

Proof: We will show that if $\overline{\beta} = \{w_1, w_2, \ldots, w_b\}$ is any given standard basis for $(W, \overline{B})$, then the number of standard bases β for (V, B, g) with $\beta \cap W = \overline{\beta}$ is equal to $q^{\frac{(a-1)b^2+b}{2}}$. And since the number of standard bases for $(W, \overline{B})$ is the same as the order of the isometry group of $(W, \overline{B})$, this will already imply the statement of the lemma.

So choose a standard basis $\{w_1, w_2, \ldots, w_b\}$ for $(W, \overline{B})$ and choose a vector v_1 from $\mathcal{S}_{w_1}$. If $b = 1$ then $\beta = \{v_1 x^k \,|\, 0 \leq k \leq a-1\}$ is a standard basis for (V, B, g) and the number of choices for v_1 is $|\mathcal{S}_{w_1}| = q^{\frac{a}{2}}$, so the lemma is true.

From now on, we may assume that $b > 1$. Notice that B is non-singular on $V_1 = \langle v_1, v_1 x, v_1 x^2, \ldots, v_1 x^{a-1} = w_1 \rangle$. For if $v = \sum_{i=0}^{a-1} \lambda_i v_1 x^i$ and j is the smallest number between 0 and $a-1$ such that $\lambda_j \neq 0$ then

$$\begin{aligned} B(v, v_1 x^{a-j-1}) &= B(\sum_{i=j}^{a-1} \lambda_i v_1 x^i, v_1 x^{a-j-1}) \\ &= B(\lambda_j v_1 x^j, v_1 x^{a-j-1}) \\ &= (-1)^j \lambda_j B(v_1, v_1 x^{a-1}) \\ &= (-1)^j \lambda_j \overline{B}(w_1, w_1) \neq 0 . \end{aligned}$$

Now, since B is non-singular on V_1, it must be also non-singular on $V_1^{\perp}$, the perpendicular space of V_1. Hence by an induction hypothesis on b, we may assume that this lemma is true for $V_1^{\perp}$. That is, the number of standard bases β_1 for $(V_1^{\perp}, B, g)$ with

$\beta_1 \cap (V_1^\perp \cap W) = \{w_2, \dots, w_b\}$ is equal to $q^{\frac{(a-1)(b-1)^2+b-1}{2}}$. Since any standard basis of $(V_1^\perp, B, g)$ together with the set $\{v_1 x^k \mid 0 \le k \le a-1\}$ forms a standard basis for (V, B, g) and since there are $|\mathcal{S}_{w_1}| = q^{(a-1)b-\frac{a}{2}+1}$ possible choices for v_1, this implies that the number of standard bases β for (V, B, g) with $\beta \cap W = \overline{\beta}$ is equal to

$$\begin{aligned} q^{\frac{(a-1)(b-1)^2+b-1}{2}} \cdot q^{(a-1)b-\frac{a}{2}+1} &= q^{\frac{(a-1)(b-1)^2+b-1+2(a-1)b-a+2}{2}} \\ &= q^{\frac{(a-1)b^2+b}{2}}, \end{aligned}$$

as we wanted. ■

Lemma 3.2.11 *Suppose that a is odd. Then the number of standard bases for (V, B, g) is*

$$q^{\frac{(a-1)b^2}{2}} \cdot |I(W, \overline{B})| \, .$$

Proof: As in the previous lemma, we will show that if $\overline{\beta} = \{w_1, w_2, \dots, w_b\}$ is any given standard basis for $(W, \overline{B})$, then the number of standard bases β for (V, B, g) with $\beta \cap W = \overline{\beta}$ is equal to $q^{\frac{(a-1)b^2}{2}}$. Since the number of standard bases for $(W, \overline{B})$ is the same as the order of the isometry group of $(W, \overline{B})$, this will already imply the statement of the lemma.

So choose a standard basis $\{w_1, w_2, \dots, w_b\}$ for $(W, \overline{B})$ and choose a pair of vectors (v_1, v_b) from $\mathcal{S}_{w_1, w_b}$. If $b = 2$ then $\beta = \{v_1 x^k \mid 0 \le k \le a-1\} \cup \{v_b x^k \mid 0 \le k \le a-1\}$ is a standard basis for (V, B, g) and the number of choices for (v_1, v_b) is $|\mathcal{S}_{w_1, w_b}| = q^{2(a-1)}$, so the lemma is true.

From now on, we may assume that $b \ge 4$. Notice that B is non-singular on $V_1 = \langle v_1 x^i, v_b x^i \mid 0 \le i \le a-1 \rangle$. For if $v = \sum_{i=1}^{a-1} \lambda_i v_1 x^i + \sum_{i=1}^{a-1} \mu_i v_b x^i$ and j is the smallest integer between 0 and $a-1$ such that $\lambda_j \ne 0$ and l is the smallest integer between 0 and $a-1$ such that $\mu_l \neq 0$ and $j \geq l$ then

$$\begin{aligned} B(v_1x^{a-l-1}, v) &= B(v_1x^{a-l-1}, \lambda_l v_1 x^l) + B(v_1x^{a-l-1}, \mu_l v_b x^l) \\ &= (-1)^{a-l-1}\lambda_l B(v_1, v_1x^{a-1}) + (-1)^{a-l-1}\mu_l B(v_1, v_bx^{a-1}) \\ &= (-1)^{a-l-1}\lambda_l \overline{B}(w_1, w_1) + (-1)^{a-l-1}\mu_l \overline{B}(w_1, w_b) \\ &= (-1)^{a-l-1}\mu_l \neq 0\,. \end{aligned}$$

In case if $j < l$,

$$\begin{aligned} B(v, v_bx^{a-j-1}) &= B(\lambda_j v_1 x^j, v_bx^{a-j-1}) \\ &= (-1)^j \lambda_j B(v_1, v_bx^{a-1}) \\ &= (-1)^j \lambda_j \overline{B}(w_1, w_b) \\ &= (-1)^j \lambda_j \neq 0\,. \end{aligned}$$

Now, since B is non-singular on V_1, it must be also non-singular on $V_1^{\perp}$, the perpendicular space of V_1. Hence by an induction hypothesis on b, we may assume that this lemma is true for $V_1^{\perp}$. That is, the number of standard bases β_1 for $(V_1^{\perp}, B, g)$ with $\beta_1 \cap (V_1^{\perp} \cap W) = \{w_2, \ldots, w_{b-1}\}$ is equal to $q^{\frac{(a-1)(b-2)^2}{2}}$. Since any standard basis of $(V_1^{\perp}, B, g)$ together with the set $\{v_1x^k \,|\, 0 \leq k \leq a-1\} \cup \{v_bx^k \,|\, 0 \leq k \leq a-1\}$ forms a standard basis for (V, B, g) and since there are $|\mathcal{S}_{w_1,w_b}| = q^{2(a-1)(b-1)}$ possible choices for (v_1, v_b), this shows that the number of standard bases β for (V, B, g) with $\beta \cap W = \overline{\beta}$ is equal to

$$\begin{aligned} q^{\frac{(a-1)(b-2)^2}{2}} \cdot q^{2(a-1)(b-1)} &= q^{\frac{(a-1)(b-2)^2+4(a-1)(b-1)}{2}} \\ &= q^{\frac{(a-1)b^2}{2}}\,, \end{aligned}$$

as we wanted. ∎

Next we show that the matrix of B under any standard basis depends only on the bilinear form $\overline{B}$ defined on W. In other words:

Lemma 3.2.12 *Suppose V_1, V_2 are vector spaces over $\mathbf{F}_q$ of dimension $d = ab$, and for $t \in 1, 2$, B_t is a non-singular symplectic form on V_t, $I(V_t, B_t)$ is the isometry group of (V_t, B_t) and g_t is a homogeneous element of $I(V_t, B_t)$ with $g^p = 1$, $x_t = g_t - 1$, $W_t = \ker(x_t)$ and $\dim_{\mathbf{F}_q} W_t = b$. Furthermore, let $\overline{B}_t$ be the bilinear form on W_t induced by g_t as in Definition 3.2.3 and let*

$$\beta_t = \{v_{ti}x_t a^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

be a standard basis for (V_t, B_t, g_t) as in Definition 3.2.7. Suppose $(W_1, \overline{B}_1)$ and $(W_2, \overline{B}_2)$ are isometric. Then the map

$$\begin{aligned} z_i : V_1 &\longrightarrow V_2 \\ v_{1i}x^k &\longmapsto v_{2i}x^k \quad (1 \leq i \leq b, 0 \leq k \leq a-1) \end{aligned}$$

is an isometry between (V_1, B_1) and (V_2, B_2).

Proof: To avoid the perhaps confusing mass of subscript indexing, let us use the following notations: $v_i = v_{1i}$, $u_i = v_{2i}$ for $1 \leq i \leq b$, $x = x_1$ and $y = x_2$. Then we need to show that

$$B_1(v_i x^k, v_j x^l) = B_2(u_i y^k, u_j y^l)$$

for all $1 \leq i, j \leq b$ and $0 \leq k, l \leq a-1$. Actually, it is enough to show that

$$B_1(v_i, v_j x^l) = B_2(u_i, u_j y^l)$$

for all $1 \leq i \leq j \leq b$ and $0 \leq l \leq a-1$, because B_1 and B_2 are symplectic bilinear forms and it is always true that

$$B_1(v_i x^k, v_j x^l) = B_1(v_i, v_j x^l(\tau(x))^k) = B_1(v_i, v_j x^l(\sum_{r=1}^{a-1}(-1)^r x^r)^k)$$

and

$$B_2(u_i y^k, u_j y^l) = B_2(u_i, u_j y^l(\tau(y))^k) = B_2(u_i, u_j y^l(\sum_{r=1}^{a-1}(-1)^r y^r)^k)\,.$$

Since $(W_1, \overline{B}_1)$ and $(W_2, \overline{B}_2)$ are isometric, it follows from the definition of standard bases (Definitions 3.2.6 and 3.2.7) that for any $1 \leq i, j \leq b$, $\overline{B}_1(v_i x^{a-1}, v_j x^{a-1}) = \overline{B}_1(u_i y^{a-1}, u_j y^{a-1})$ and hence

$$B_1(v_i, v_j x^{a-1}) = \overline{B}_1(v_i x^{a-1}, v_j x^{a-1}) = \overline{B}_2(u_i y^{a-1}, u_j y^{a-1}) = B_2(u_i, u_j y^{a-1}) .$$

Also, from the definition of standard bases,

$$B_1(v_i, v_j x^l) = 0 = B_2(u_i, u_j y^l)$$

whenever $l < a-1$ and either $i \leq j$ or $i = j$ and l is an odd number. Finally, we need to show that for any $1 \leq i \leq b$ and $0 \leq l < \frac{a-1}{2}$,

$$B_1(v_i, v_i x^{2l}) = B_2(u_i, u_i y^{2l}) .$$

By an induction hypothesis on l we may assume that $B_1(v_i, v_i^k) = B_2(u_i, u_i y^k)$ for all $k \geq 2l+1$. Then by Lemma 3.2.2, there is a polynomial $h_l(t) \in \mathbf{Z}[t]$ of degree $2l+1$ such that

$$B_1(v_i, v_i x^{2l}) = B_1(v_i, v_i\, h_l(x)) \quad \text{and} \quad B_2(u_i, u_i y^{2l}) = B_2(u_i, u_i\, h_l(y)) .$$

By our induction hypothesis $B_1(v_i, v_i\, h_l(x)) = B_2(u_i, u_i\, h_l(y))$, therefore $B_1(v_i, v_i x^{2l}) = B_2(u_i, u_i y^{2l})$ and this completes the proof. ■

Now we are ready to prove that the bilinear form $\overline{B}$ on W characterizes the conjugacy class of g in $I(V, B)$.

Theorem 3.2.13 *Let $g, h \in I(V, B)$ homogeneous elements of order p, $x = g - 1$, $y = h - 1$ and let $\overline{B}_g$ and $\overline{B}_h$ be the bilinear forms on $W_g = \ker x$ and $W_h = \ker y$ induced by g and h, respectively. Then g and h are conjugate in $I(V, B)$ if and only if there is an isometry between $(W_g, \overline{B}_g)$ and $(W_h, \overline{B}_h)$.*

Proof: First assume that g and h are conjugate in $I(V,B)$ that is, $h = z^{-1}gz$ for some $z \in I(V,B)$. Then of course, $y = z^{-1}xz$ and $W_h = W_g z$. (For if $v \in W_g$ then $(vz)y = (vz)z^{-1}xz = vxz = 0z = 0$.) In fact the map

$$\begin{aligned} \varphi : W_g &\longrightarrow W_h \\ v &\longmapsto vz \end{aligned}$$

is an isometry between W_g and W_h, as for any $u, v \in V$

$$\begin{aligned} \overline{B}_h(ux^{a-1}z, vx^{a-1}z) &= \overline{B}_h(uz(z^{-1}x^{a-1}z), vz(z^{-1}x^{a-1}z)) \\ &= \overline{B}_h(uzy^{a-1}, vzy^{a-1}) \\ &= B(uz, vzy^{a-1}) \\ &= B(uz, vx^{a-1}z) \\ &= B(u, vx^{a-1}) \\ &= \overline{B}_g(ux^{a-1}, vx^{a-1})\,. \end{aligned}$$

To prove the other direction, assume that $(W_g, \overline{B}_g)$ and $(W_h, \overline{B}_h)$ are isometric and let $\{v_1, v_2, \ldots, v_b\}$ and $\{u_1, u_2, \ldots, u_b\}$ be ordered subsets of V such that $\beta_g = \{v_i x^k \,|\, 1 \leq i \leq b, 0 \leq k \leq a-1\}$ and $\beta_h = \{u_i y^k \,|\, 1 \leq i \leq b, 0 \leq k \leq a-1\}$ are standard bases for (V, B, g) and (V, B, h), respectively, as in Definition 3.2.7. Define $z \in GL(V)$ to be the map

$$\begin{aligned} z : V &\longrightarrow V \\ v_i x^k &\longmapsto u_i x^k \quad (1 \leq i \leq b\,, 0 \leq k \leq a-1). \end{aligned}$$

Then certainly $h = z^{-1}gz$ and $y = z^{-1}xz$, and as we proved it in Lemma 3.2.12, $z \in I(V,B)$. ∎

Theorem 3.2.14

$$|C_{I(V,B)}(g)| = \begin{cases} q^{\frac{(a-1)b^2+b}{2}} \cdot |I(W, \overline{B})|, & \textit{if } a \textit{ is even;} \\ q^{\frac{(a-1)b^2}{2}} \cdot |I(W, \overline{B})|, & \textit{if } a \textit{ is odd.} \end{cases}$$

Proof: According to Lemma 3.2.12 if $\{v_i \,|\, 1 \leq i \leq b\}$ and $\{u_i \,|\, 1 \leq i \leq b\}$ are ordered subsets of V such that

$$\beta_1 = \{v_i x^k \,|\, 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

and

$$\beta_2 = \{u_i x^k \,|\, 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

are standard bases for (V, B, g) then there is an element z in $C_{I(V,B)}(g)$, the centralizer of g in $I(V, B)$, such that $v_i x^k z = u_i x^k$ for all i and k. In other words, $C_{I(V,B)}(g)$ acts transitively (and thus regularly) on the standard bases of (V, B, g). This means that the order of $C_{I(V,B)}(g)$ is equal to the number of standard bases for (V, B, g), which number is calculated in Lemmas 3.2.10 and 3.2.11. ∎

Definition 3.2.15 *Define a real number $\rho(V, B, g)$ for the triple (V, B, g) as follows.*

$$\rho(V,B,g) = \begin{cases} 2, & \textit{if } a \textit{ is even and } b \textit{ is odd;} \\ \frac{2q^{\frac{b}{2}}}{q^{\frac{b}{2}}+1}, & \textit{if } a \textit{ and } b \textit{ are even and } (W,\overline{B}) \textit{ is of type } +; \\ \frac{2q^{\frac{b}{2}}}{q^{\frac{b}{2}}-1}, & \textit{if } a \textit{ and } b \textit{ are even and } (W,\overline{B}) \textit{ is of type } -; \\ q^{\frac{b}{2}}, & \textit{if } a \textit{ is odd.} \end{cases}$$

Theorem 3.2.16

$$|C_{I(V,B)}(g)| = q^{\frac{ab^2}{2}} \prod_{\substack{1 \leq k \leq b \\ k \text{ even}}} \left(1 - \frac{1}{q^k}\right) \cdot \rho(V,B,g)\,.$$

Proof: If a is even and $b = 2l+1$ then

$$\begin{aligned} |I(W,\overline{B})| &= |\mathrm{O}_{2l+1}(q)| \\ &= 2q^{l^2}(q^2-1)(q^4-1)\cdots(q^{2l-1}-1) \\ &= 2q^{l(2l+1)} \prod_{k=1}^{l} \left(1 - \frac{1}{q^{2k}}\right) \\ &= 2q^{\frac{b^2-b}{2}} \prod_{\substack{1 \leq k \leq b \\ k \text{ even}}} \left(1 - \frac{1}{q^k}\right). \end{aligned}$$

If a is even and $b = 2l$ and $(W\overline{B})$ is of type ϵ then

$$\begin{aligned}
|I(W,\overline{B})| &= |\mathrm{O}^{\epsilon}_{2l}(q)| \\
&= 2q^{l(l-1)}(q^2-1)(q^4-1)\cdots(q^{2l-1})\frac{1}{q^l+\epsilon 1} \\
&= 2q^{l(2l-1)}\prod_{k=1}^{l}\left(1-\frac{1}{q^{2k}}\right)\cdot\frac{q^l}{q^l+\epsilon 1} \\
&= q^{\frac{b^2-b}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g)\,.
\end{aligned}$$

If a is odd, then $b = 2l$ for some integer l and

$$\begin{aligned}
|I(W,\overline{B})| &= |\mathrm{Sp}_{2l}(q)| \\
&= q^{l^2}(q^2-1)(q^4-1)\cdots(q^{2l-1}-1) \\
&= q^{l(2l+1)}\prod_{k=1}^{l}\left(1-\frac{1}{q^{2k}}\right) \\
&= q^{\frac{b^2}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g)\,.
\end{aligned}$$

The rest follows from Theorem 3.2.14: If a is even then

$$\begin{aligned}
|C_{I(V,B)}(g)| &= q^{\frac{(a-1)b^2+b}{2}}\cdot|I(W,\overline{B})| \\
&= q^{\frac{(a-1)b^2+b}{2}}\cdot q^{\frac{b^2-b}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g) \\
&= q^{\frac{ab^2}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g)\,,
\end{aligned}$$

and if a is odd then

$$\begin{aligned}
|C_{I(V,B)}(g)| &= q^{\frac{(a-1)b^2}{2}}\cdot|I(W,\overline{B})| \\
&= q^{\frac{(a-1)b^2}{2}}\cdot q^{\frac{b^2}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g) \\
&= q^{\frac{ab^2}{2}}\prod_{\substack{1\le k\le b\\ k \text{ even}}}\left(1-\frac{1}{q^k}\right)\cdot\rho(V,B,g)\,.
\end{aligned}$$

This completes the proof. ■

According to Theorem 3.2.13 if a is odd then in $I(V,B)$ there is only one conjugacy class of homogeneous elements g with the properties that $g^p = 1$ and $\dim_{\mathbf{F}_q} \ker(g-1) = b$. (Of course, assuming that there exist such elements in $I(V,B)$.) And this is true because there is only one symplectic form on vector spaces of dimension b over $\mathbf{F}_q$, up to isometry. However, this is not the case for symmetric forms in dimension b, so it is a natural question to ask whether the homogeneous elements g in $I(V,B)$ with $g^p = 1$ and $\dim_{\mathbf{F}_q} \ker(g-1) = b$ form one or two conjugacy classes in $I(V,B)$, when a is an even number. We finish Section 3.2 by giving an answer to this question.

Theorem 3.2.17 *Let V be a vector space of dimension d over $\mathbf{F}_q$ equipped with a non-singular symplectic form B and let $I(V,B)$ be the isometry group of B. Furthermore, let $d = a \cdot b$ with $1 \leq a \leq p$ and let $\mathcal{C}$ be the set of homogeneous elements g in $I(V,B)$ with $g^p = 1$ and $\dim_{\mathbf{F}_q} \ker(g-1) = b$. Assume that $\mathcal{C}$ is non-empty. Then $\mathcal{C}$ is a single conjugacy class in $I(V,B)$ if a is odd and $\mathcal{C}$ is a union of two conjugacy classes in $I(V,B)$ if a is even.*

Proof: Once again, this theorem immediately follows from Theorem 3.2.13 if a is odd, as we already explained it before. To prove the theorem in the case when a is even, we just need to show that both symmetric forms in dimension b can occur as induced forms $\overline{B}_g$ on the kernel of $g-1$ for some g in $\mathcal{C}$.

Choose an element $g \in \mathcal{C}$ and as always, let $x = g-1$ and $W = \ker(x) = Vx^{a-1}$. Also, let $\beta = \{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$ be a standard basis for (V,B,g). Then it follows that the subspaces $V_i = \langle v_i x^k \mid 0 \leq k \leq a-1 \rangle$ for $i = 1,2,\ldots,b$ are perpendicular to each other. (See the proof of Lemma 3.2.10.) Define a new symplectic form B' on V so that

$$B'(u,v) = \begin{cases} B(u,v), & \text{if } u,v \in V_i \text{ for some } 1 \leq i \leq b-1\ ; \\ \delta B(u,v), & \text{if } u,v \in V_b\ . \end{cases}$$

Recall that δ is a fixed quadratic non-residue in $\mathbf{F}_q$. Obviously, B' is a non-singular symplectic form on V, $g \in I(V, B')$ and the induced symmetric form $\overline{B}'$ on W is not isometric to B. Now, $I(V, B)$ and $I(V, B')$ are isometric, both being a non-singular symplectic form on the same vector space. Say $z \in \mathrm{GL}(V)$ is an isometry from (V, B') to (V, B) that is, $B(uz, vz) = B'(u, v)$ for all $u, v \in V$. Then $z^{-1}gz \in I(V, B)$ with its induced symmetric form $\overline{B}_{z^{-1}gz}$ on $\ker(z^{-1}gz - 1) = Wz$ isometric to $\overline{B}'$. Hence $z^{-1}gz$ is an element of $\mathcal{C}$ that is not conjugate to g in $I(V, B)$. ■

3.3 Elements of Order p with Homogeneous Action in GU Groups

In this section V is a vector space of dimension d over $\mathbf{F}_{q^2}$ ($q = p^f$) equipped with a non-singular unitary form B, $I(V, B)$ is the isometry group of (V, B) and g is an element of $I(V, B)$ with $g^p = 1$, acting homogeneously on V. That is, the $\mathbf{F}_{q^2}\langle g\rangle$-module V decomposes into a direct sum of isomorphic indecomposable $\mathbf{F}_{q^2}$-modules. Say $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$ where each V_i is an indecomposable $\mathbf{F}_{q^2}$-module of dimension a. Then of course, $a \leq p$ and $ab = d$. Also, let δ be a fixed nonzero element of $\mathbf{F}_{q^2}$ with $\delta^q = -\delta$. If $p = 2$ then let $\delta = 1$. We will use the notation $\bar{\alpha}$ for the conjugate α^q of any element α in $\mathbf{F}_{q^2}$.

Like in the previous section, let τ be the anti-isomorphism of $\mathrm{End}_{\mathbf{F}_{q^2}}(V)$ with the property that

$$B(u\varphi, v) = B(u, v\tau(\varphi))$$

for all u, v in V and φ in $\mathrm{End}_{\mathbf{F}_{q^2}}(V)$.

Also let $x = g - 1$, so $x^a = 0$ and like in the previous section it is true that

$$\begin{aligned} \tau(x) &= \sum_{k=1}^{a-1}(-1)^k x^k \\ &= -x - x\tau(x) \end{aligned}$$

and $B(ux^k, vx^l) = 0$ whenever $k + l \geq a$ and $B(ux^k, vx^l) = (-1)^k B(u, vx^{a-1})$ whenever $k + l = a - 1$.

Let W be the kernel of x, so W is a b-dimensional subspace of V that is determined by g. As in the previous section, we will introduce a non-singular form $\overline{B}$ on W, but this time it will be a unitary form and the definition of $\overline{B}$ will depend on the parity of a. Then we will show that the conjugacy class of g in $I(V, B)$ is the intersection of $I(V, B)$ with the conjugacy class of g in $\mathrm{GL}(V)$. Finally, we will give a formula for the order of the centralizer of g in $I(V, B)$.

Definition 3.3.1 *Define $\overline{B}$ as follows.*

$$\overline{B} : W \times W \longrightarrow \mathbf{F}_{q^2}$$

$$\overline{B}(ux^{a-1}, vx^{a-1}) = \begin{cases} B(u, vx^{a-1}), & \textit{if } a \textit{ is odd;} \\ \delta B(u, vx^{a-1}), & \textit{if } a \textit{ is even.} \end{cases}$$

Lemma 3.3.2 *$\overline{B}$ is a well-defined non-singular unitary form on W.*

Proof: If $u_1x^{a-1} = ux^{a-1}$ and $v_1x^{a-1} = vx^{a-1}$ then

$$\begin{aligned} B(u_1, v_1x^{a-1}) &= B(u, vx^{a-1}) + B(u_1 - u, vx^{a-1}) \\ &= B(u, vx^{a-1}) + (-1)^{a-1}B((u_1 - u)x^{a-1}, v) \\ &= B(u, vx^{a-1}) + (-1)^{a-1}B(0, v) \\ &= B(u, vx^{a-1}) . \end{aligned}$$

Also,

$$\begin{aligned} B(v, ux^{a-1}) &= (-1)^{a-1}B(vx^{a-1}, u) \\ &= (-1)^{a-1}\overline{B(u, vx^{a-1})} \end{aligned}$$

so if a is odd then

$$\overline{B}(vx^{a-1}, ux^{a-1}) = B(v, ux^{a-1}) = \overline{B(u, vx^{a-1})} = \overline{\overline{B}(ux^{a-1}, vx^{a-1})}$$

and if a is even then

$$\overline{B}(vx^{a-1}, ux^{a-1}) = \delta B(v, ux^{a-1}) = -\delta\overline{B(u, vx^{a-1})} =$$

$$= \overline{\delta B(u, vx^{a-1})} = \overline{\overline{B}(ux^{a-1}, vx^{a-1})}\ .$$

Finally, the non-singularity of $\overline{B}$ on W follows obviously from the non-singularity of B on V. ■

Definition 3.3.3 *Let $\overline{\beta}$ be an ordered basis for W. We say that $\overline{\beta}$ is a* **standard basis** *for $(W, \overline{B})$ if*

$$\overline{B}(w_i, w_j) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

Let $\{v_1, v_2, \ldots, v_b\}$ be an ordered subset of V such that

$$\beta = \{v_i x^k \,|\, 1 \leq i \leq b,\ 0 \leq k \leq a-1\}$$

is a basis for V. We say that β together with the ordering of $\{v_1, v_2, \ldots, v_b\}$ is a **standard basis** *for (V, B, g) if*

1. *$\{v_i x^{a-1} \,|\, 1 \leq i \leq b\}$ is a standard basis for $(W, \overline{B})$,*
2. *$B(v_i x^k, v_j x^l) = 0$ whenever $i \neq j$,*
3. *One of the following holds.*
   - *(a) The number a is an odd integer, $B(v_i, v_i x^k) \in \mathbf{F}_q$ for all i and k, and $B(v_i, v_i x^k) = 0$ whenever k is an even number strictly less than $a-1$.*
   - *(b) a is an even integer, p is an odd prime, $B(v_i, v_i x^k) \in \delta\mathbf{F}_q$ for all i and k, and $B(v_i, v_i x^k) = 0$ whenever k is an odd number strictly less than $a-1$.*
   - *(c) $a = p = 2$ and $B(v_i, v_i) = 0$ for all $1 \leq i \leq b$.*

Lemma 3.3.4 *Suppose that a is odd and let $w \in W$ be any nonzero vector. Define $\mathcal{S}_w$ to be the set of all vectors v in V such that $vx^{a-1} = w$, $B(v, vx^k) = 0$ for every even number k with $0 \le k < a-1$ and $B(v, vx^k) \in \mathbf{F}_q$ for every $0 \le k \le a-1$. Then*

$$|\mathcal{S}_w| = q^{(a-1)(2b-1)} .$$

Proof: Notice that $B(v, vx^{a-1}) = \overline{B}(vx^{a-1}, vx^{a-1}) \in \mathbf{F}_q$ for any $v \in V$, so actually we could omit the condition $B(v, vx^{a-1}) \in \mathbf{F}_q$ from the definition of $\mathcal{S}_w$.

If $a = 1$ then $q^{(a-1)(2b-1)} = 1$ and $\mathcal{S}_w = \{w\}$, so from now on, we may assume that $a \ge 3$ (and hence p is an odd prime). Let

$$W_1 = \{v \in V \,|\, vx^{a-1} = w\}$$

and define the maps φ_i for $1 \le i \le a-1$ and sets W_i for $2 \le i \le a$ as follows. For any $1 \le i \le a-1$ let

$$\begin{aligned} \varphi_i : W_i &\longrightarrow \mathbf{F}_{q^2} \\ v &\longmapsto B(v, vx^{a-i-1}) \\ W_{i+1} &= \begin{cases} \{v \in W_i \,|\, \varphi_i(v) = 0\}, & \text{if } i \text{ is even;} \\ \{v \in W_i \,|\, \varphi_i(v) \in \mathbf{F}_q\}, & \text{if } i \text{ is odd.} \end{cases} \end{aligned}$$

Since $|W_1| = q^{2(a-1)b}$ and $\mathcal{S}_w = W_a$, it will be enough to show that $|W_{l+1}| = \frac{1}{q}|W_l|$ for any $1 \le l \le a-1$.

First assume that l is odd and let v be any vector in W_l. Then for any $v' \in V$, $v + v'x^l$ is also an element of W_l because $(v + v'x^l)x^{a-1} = w$ and for any $1 \le i \le l-1$,

$$\varphi_i(v + v'x^l) = B(v + v'x^l, (v + v'x^l)x^{a-i-1}) =$$

$$= B(v, vx^{a-i-1}) = \varphi_i(v) ,$$

as $a+l-i-1 \geq a$. Furthermore,

$$\begin{aligned}
\varphi_l(v+v'x^l) &= B(v+v'x^l,(v+v'x^l)x^{a-l-1}) \\
&= B(v,vx^{a-l-1})+B(v,v'x^{a-1})+B(v'x^l,vx^{a-l-1}) \\
&= B(v,vx^{a-l-1})+B(v,v'x^{a-1})-B(v',vx^{a-1}) \\
&= \varphi_l(v)+\overline{B}(vx^{a-1},v'x^{a-1})-\overline{\overline{B}(vx^{a-1},v'x^{a-1})} \\
&= \varphi_l(v)+\overline{B}(w,v'x^{a-1})-\overline{\overline{B}(w,v'x^{a-1})}\,.
\end{aligned}$$

Notice that the map

$$\begin{aligned}
\alpha_l : Vx^l &\longrightarrow \delta\mathbf{F}_q \\
v'x^l &\longmapsto \overline{B}(w,v'x^{a-1})-\overline{\overline{B}(w,v'x^{a-1})}
\end{aligned}$$

is a well-defined non-trivial $\mathbf{F}_q$-linear map, and

$$v+v'x^l \in W_{l+1} \Longleftrightarrow \alpha_l(v'x^l)=\frac{1}{2}[\overline{\varphi_l(v)}-\varphi_l(v)]\,,$$

so

$$|W_{l+1}\cap\{v+Vx^l\}|=\frac{1}{q}|\{v+Vx^l\}|\,.$$

This is true for any $v \in W_l$, therefore

$$|W_{l+1}|=\frac{1}{q}|W_l+Vx^l|=\frac{1}{q}|W_l|\,.$$

Next, assume that l is even and let v be any vector in W_l. Then by the way we defined W_l, $B(v,vx^i)\in\mathbf{F}_q$ for any $i \geq a-l$. Since $a-l-1$ is an even integer in this case, by Lemma 3.2.2 there is a polynomial $h(t)\in\mathbf{Z}[t]$ of degree $a-l$ such that

$$\varphi_l(v)=B(v,vx^{a-l-1})=(-1)^{\frac{a-l-1}{2}}B(vx^{\frac{a-l-1}{2}},vx^{\frac{a-l-1}{2}})+B(v,v\,h(x))\,.$$

This shows that $\varphi_l(v)\in\mathbf{F}_q$, and this is true for any vector v in W_l.

Notice that for any $v'\in V$, $v+v'x^l$ is also an element of W_l because $(v+v'x^l)x^{a-1}=w$ and for any $1\leq i\leq l-1$,

$$\varphi_i(v+v'x^l)=B(v+v'x^l,(v+v'x^l)x^{a-i-1})=$$

$$= B(v, vx^{a-i-1}) = \varphi_i(v) ,$$

as $a + l - i - 1 \geq a$. Furthermore,

$$\begin{aligned}
\varphi_l(v + v'x^l) &= B(v + v'x^l, (v + v'x^l)x^{a-l-1}) \\
&= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) + B(v'x^l, vx^{a-l-1}) \\
&= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) + B(v', vx^{a-1}) \\
&= \varphi_l(v) + \overline{B}(vx^{a-1}, v'x^{a-1}) + \overline{\overline{B}(vx^{a-1}, v'x^{a-1})} \\
&= \varphi_l(v) + \overline{B}(w, v'x^{a-1}) + \overline{\overline{B}(w, v'x^{a-1})} .
\end{aligned}$$

Now, that the map

$$\begin{aligned}
\alpha_l : Vx^l &\longrightarrow \mathbf{F}_q \\
v'x^l &\longmapsto \overline{B}(w, v'x^{a-1}) + \overline{\overline{B}(w, v'x^{a-1})}
\end{aligned}$$

is a well-defined non-trivial $\mathbf{F}_q$-linear map and

$$v + v'x^l \in W_{l+1} \Longleftrightarrow \alpha_l(v'x^l) = -\varphi_l(v) ,$$

so

$$|W_{l+1} \cap \{v + Vx^l\}| = \frac{1}{q}|\{v + Vx^l\}| .$$

This is true for any $v \in W_l$, therefore

$$|W_{l+1}| = \frac{1}{q}|W_l + Vx^l| = \frac{1}{q}|W_l| .$$

This completes the proof of the lemma. ■

Lemma 3.3.5 *Suppose that a is even and let $w \in W$ be any nonzero vector. Define $\mathcal{S}_w$ to be the set of all vectors v in V such that $vx^{a-1} = w$, $B(v, vx^k) = 0$ for every odd number k with $0 \leq k < a - 1$ and either p is odd and $B(v, vx^k) \in \delta\mathbf{F}_q$ for every $0 \leq k \leq a - 1$ or $p = 2$ and $B(v, v) = 0$. Then*

$$|\mathcal{S}_w| = q^{(a-1)(2b-1)} .$$

Proof: Notice that $B(v, vx^{a-1}) = \delta^{-1}\overline{B}(vx^{a-1}, vx^{a-1}) \in \delta\mathbf{F}_q$ for any $v \in V$, so actually we could omit the condition $B(v, vx^{a-1}) \in \delta\mathbf{F}_q$ from the definition of $\mathcal{S}_w$.

Let $W_1 = \{v \in V \,|\, vx^{a-1} = w\}$ and define the maps φ_i for $1 \leq i \leq a-1$ and sets W_i for $2 \leq i \leq a$ as follows. For any $1 \leq i \leq a-1$ let

$$\begin{aligned} \varphi_i : W_i &\longrightarrow \mathbf{F}_{q^2} \\ v &\longmapsto B(v, vx^{a-i-1}) \end{aligned}$$

$$W_{i+1} = \begin{cases} \{v \in W_i \,|\, \varphi_i(v) = 0\}, & \text{if } p \text{ and } i \text{ are odd;} \\ \{v \in W_i \,|\, \varphi_i(v) \in \delta\mathbf{F}_q\}, & \text{if } p \text{ is odd and } i \text{ is even;} \\ \{v \in W_i \,|\, \varphi_i(v) = 0\}, & \text{if } p = 2 \text{ and } i = 1. \end{cases}$$

Since $|W_1| = q^{2(a-1)b}$ and $\mathcal{S}_w = W_a$, it will be enough to show that $|W_{l+1}| = \frac{1}{q}|W_l|$ for any $1 \leq l \leq a-1$.

First assume that l is odd and let v be any vector in W_l. Then for any $v' \in V$, $v + v'x^l$ is also an element of W_l because $(v + v'x^l)x^{a-1} = w$ and for any $1 \leq i \leq l-1$,

$$\varphi_i(v + v'x^l) = B(v + v'x^l, (v + v'x^l)x^{a-i-1}) =$$

$$= B(v, vx^{a-i-1}) = \varphi_i(v)\,,$$

as $a + l - i - 1 \geq a$. Furthermore,

$$\begin{aligned} \varphi_l(v + v'x^l) &= B(v + v'x^l, (v + v'x^l)x^{a-l-1}) \\ &= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) + B(v'x^l, vx^{a-l-1}) \\ &= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) - B(v', vx^{a-1}) \\ &= \varphi_l(v) + \delta^{-1}[\overline{B}(vx^{a-1}, v'x^{a-1}) - \overline{\overline{B}(vx^{a-1}, v'x^{a-1})}] \\ &= \varphi_l(v) + \delta^{-1}[\overline{B}(w, v'x^{a-1}) - \overline{\overline{B}(w, v'x^{a-1})}]\,. \end{aligned}$$

Notice that the map

$$\begin{aligned} \alpha_l : Vx^l &\longrightarrow \mathbf{F}_q \\ v'x^l &\longmapsto \delta^{-1}[\overline{B}(w, v'x^{a-1}) - \overline{\overline{B}(w, v'x^{a-1})}] \end{aligned}$$

is a well-defined non-trivial $\mathbf{F}_q$-linear map and

$$v + v'x^l \in W_{l+1} \iff \alpha_l(v'x^l) = -\frac{1}{2}[\varphi_l(v) + \overline{\varphi_l(v)}]$$

if the characteristic is odd and

$$v + v'x^l \in W_{l+1} \iff \alpha_l(v'x^l) = -\varphi_l(v)$$

if the characteristic is even (and in that case, actually $l = 1$ and $\varphi_l(v) = B(v, v)$ for all v). This shows that

$$|W_{l+1} \cap \{v + Vx^l\}| = \frac{1}{q}|\{v + Vx^l\}| \, .$$

This is true for any $v \in W_l$, therefore

$$|W_{l+1}| = \frac{1}{q}|W_l + Vx^l| = \frac{1}{q}|W_l| \, .$$

Next, assume that l is even and now we can also assume that the characteristic is odd. Let v be any vector in W_l. Then because of the way we defined W_l, $B(v, vx^i) \in \delta\mathbf{F}_q$ for any $i \geq a - l$. Also

$$\begin{aligned}
\varphi_l(v) + \overline{\varphi_l(v)} &= B(v, vx^{a-l-1}) + \overline{B(v, vx^{a-l-1})} \\
&= B(v, vx^{a-l-1}) + B(vx^{a-l-1}, v) \\
&= B(v, vx^{a-l-1}) + B(v, v\tau(x)^{a-l-1}) \\
&= B(v, v[x^{a-l-1} + \tau(x)^{a-l-1}]) \, .
\end{aligned}$$

Here, since $a - l - 1$ is an odd number,

$$x^{a-l-1} + \tau(x)^{a-l-1} = x^{a-l-1} + (\sum_{k=1}^{a-1}(-1)^k x^k)^{a-l-1}$$

is a polynomial of x of degree at least $a - l$, therefore

$$B(v, v[x^{a-l-1} + \tau(x)^{a-l-1}]) \in \delta\mathbf{F}_q$$

that is, $\varphi_l(v) + \overline{\varphi_l(v)} \in \delta\mathbf{F}_q$. This means that $\varphi_l(v) \in \delta\mathbf{F}_q$, and this is true for any vector v in W_l.

Like with all the other cases (regarding the parities of a and l), it is also true that for any $v' \in V$ that $v + v'x^l$ is also an element of W_l, because $(v + v'x^l)x^{a-1} = vx^{a-1} = w$ and for any $1 \leq i \leq l-1$,

$$\varphi_i(v + v'x^l) = B(v + v'x^l, (v + v'x^l)x^{a-i-1}) =$$

$$= B(v, vx^{a-i-1}) = \varphi_i(v) ,$$

as $a + l - i - 1 \geq a$. Furthermore,

$$\begin{aligned}
\varphi_l(v + v'x^l) &= B(v + v'x^l, (v + v'x^l)x^{a-l-1}) \\
&= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) + B(v'x^l, vx^{a-l-1}) \\
&= B(v, vx^{a-l-1}) + B(v, v'x^{a-1}) + B(v', vx^{a-1}) \\
&= \varphi_l(v) + \delta^{-1}[\overline{B}(vx^{a-1}, v'x^{a-1}) + \overline{\overline{B}(vx^{a-1}, v'x^{a-1})}] \\
&= \varphi_l(v) + \delta^{-1}[\overline{B}(w, v'x^{a-1}) + \overline{\overline{B}(w, v'x^{a-1})}] .
\end{aligned}$$

Notice that the map

$$\begin{aligned}
\alpha_l : Vx^l &\longrightarrow \delta\mathbf{F}_q \\
v'x^l &\longmapsto \delta^{-1}[\overline{B}(w, v'x^{a-1}) + \overline{\overline{B}(w, v'x^{a-1})}]
\end{aligned}$$

is a well-defined non-trivial $\mathbf{F}_q$-linear map and

$$v + v'x^l \in W_{l+1} \Longleftrightarrow \alpha_l(v'x^l) = -\varphi_l(v) ,$$

so

$$|W_{l+1} \cap \{v + Vx^l\}| = \frac{1}{q}|\{v + Vx^l\}| .$$

This is true for any $v \in W_l$, therefore

$$|W_{l+1}| = \frac{1}{q}|W_l + Vx^l| = \frac{1}{q}|W_l| .$$

This completes the proof of the lemma. ■

Lemma 3.3.6 *The number of standard bases for* (V, B, g) *is*

$$q^{(a-1)b^2} \cdot |I(W, \overline{B})| = q^{ab^2} \cdot \prod_{k=1}^{b} \left(1 - \frac{(-1)^k}{q^k}\right) .$$

Proof: We will show that if $\overline{\beta} = \{w_1, w_2, \dots, w_b\}$ is any given standard basis for $(W, \overline{B})$, then the number of standard bases $\beta = \{v_i x^k \mid 1 \le i \le b, 0 \le k \le a-1\}$ for (V, B, g) with $v_i x^{a-1} = w_i$ $(i = 1, 2, \dots, b)$ is equal to $q^{(a-1)b^2}$. And since the number of standard bases for $(W, \overline{B})$ is the same as the order of the isometry group of $(W, \overline{B})$, this will already imply the statement of the lemma.

So choose a standard basis $\{w_1, w_2, \dots, w_b\}$ for $(W, \overline{B})$ and choose a vector v_1 from $\mathcal{S}_{w_1}$. If $b = 1$ then $\beta = \{v_1 x^k \mid 0 \le k \le a-1\}$ is a standard basis for (V, B, g) and the number of choices for v_1 is $|\mathcal{S}_{w_1}| = q^{a-1}$, so the lemma is true.

From now on, we may assume that $b > 1$. Notice that B is non-singular on $V_1 = \langle v_1, v_1 x, v_x^2, \dots, v_1 x^{a-1} = w_1 \rangle$. For if $v = \sum_{i=0}^{a-1} \lambda_i v_1 x^i$ and j is the smallest integer between 0 and $a - 1$ such that $\lambda_j \ne 0$ then

$$\begin{aligned}
B(v, v_1 x^{a-j-1}) &= B(\sum_{i=j}^{a-1} \lambda_i v_1 x^i, v_1 x^{a-j-1}) \\
&= B(\lambda_j v_1 x^j, v_1 x^{a-j-1}) \\
&= (-1)^j \lambda_j B(v_1, v_1 x^{a-1}) \\
&= (-1)^j \lambda_j \overline{B}(w_1, w_1) \\
&= (-1)^j \lambda_j \ne 0 .
\end{aligned}$$

Now, since B is non-singular on V_1, it must be also non-singular on $V_1^\perp$, the perpendicular space of V_1. Hence by an induction hypothesis on b, we may assume that this lemma is true for $V_1^\perp$ that is, the number of standard bases $\beta_1 = \{v_i x^k \mid 2 \le i \le b, 0 \le k \le a-1\}$ for $(V_1^\perp, B, g)$ with $v_i x^{a-1} = w_i$ $(2 \le i \le a-1)$ is equal to $q^{(a-1)(b-1)^2}$. Since any standard basis of $(V_1^\perp, B, g)$ together with the set $\{v_1 x^k \mid 0 \le k \le a-1\}$ forms a standard basis for (V, B, g) and since there are $|\mathcal{S}_{w_1}| = q^{(a-1)(2b-1)}$ possible choices for

v_1, this shows that the number of standard bases $\beta = \{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$ for (V, B, g) with $v_i x^{a-1} = w_i$ $(i = 1, 2, \ldots, b)$ is equal to

$$q^{(a-1)(b-1)^2} \cdot q^{(a-1)(2b-1)} = q^{(a-1)b^2},$$

as we wanted. ■

Next we show that the matrix of B under any standard basis is always the same. In other words:

Lemma 3.3.7 *Suppose V_1, V_2 are vector spaces over $\mathbf{F}_{q^2}$ of dimension $d = ab$, and for $t \in \{1,2\}$, B_t is a non-singular unitary form on V_t, $I(V_t, B_t)$ is the isometry group of (V_t, B_t) and g_t is a homogeneous element of $I(V_t, B_t)$ with $g_t^p = 1$, $x_t = g_t - 1$, $W_t = \ker(x_t)$ and $\dim_{\mathbf{F}_{q^2}}(W_t) = b$. Furthermore, let $\overline{B}_t$ be the bilinear form on W_t induced by g_t as in Definition 3.3.1 and let*

$$\beta_t = \{v_t i x_t^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

be a standard basis for (V_t, B_t, g_t) as in Definition 3.3.3. Then the map

$$\begin{aligned} z : V_1 &\longrightarrow V_2 \\ v_{1i} x^k &\longmapsto v_{2i} x^k \quad (1 \leq i \leq b, 0 \leq k \leq a-1) \end{aligned}$$

is an isometry from (V_1, B_1) to (V_2, B_2).

Proof: Like in the proof of Lemma 3.2.12, it is worth simplifying a little bit on the notation. Let $v_i = v_{1i}$, $u_i = v_{2i}$ for $1 \leq i \leq b$, $x = x_1$ and $y = x_2$. Then we need to show that

$$B_1(v_i x^k, v_j x^l) = B_2(u_i y^k, u_j y^l)$$

for all $1 \leq i, j \leq b$ and $0 \leq k, l \leq a-1$. Since by the definition of standard bases (see Definition 3.3.3), $B_1(v_i x^k, v_j x^l) = 0 = B_2(u_i y^k, u_j y^l)$ whenever $i \neq j$, and since for any $1 \leq i \leq b$ and $0 \leq k, l \leq a-1$,

$$B_1(v_i x^k, v_i x^l) = B_1(v_i, v_i x^l \tau(x)^k) = B_1(v_i, v_i x^l (\sum_{j=1}^{a-1} (-1)^j x^j)^k)$$

and

$$B_2(u_iy^k, u_iy^l) = B_2(u_i, u_iy^l\tau(y)^k) = B_2(u_i, u_iy^l(\sum_{j=1}^{a-1}(-1)^jy^j)^k) ,$$

it will be enough to show that

$$B_1(v_i, v_ix^l) = B_2(u_i, u_iy^l)$$

for all $1 \le i \le b$ and $0 \le l \le a-1$. We will do this by way of contradiction.

Suppose $B_1(v_i, v_ix^l) \neq B_2(u_i, u_iy^l)$ for some i and l and we may assume that $B_1(v_i, v_ix^k) = B_2(u_i, u_iy^k)$ for any $k \ge l+1$. Of course, $l \le a-2$ since

$$B_1(v_i, v_ix^{a-1}) = \overline{B}_1(v_ix^{a-1}, v_ix^{a-1}) = 1 =$$

$$= \overline{B}_2(u_iy^{a-1}, u_iy^{a-1}) = B_2(u_i, u_iy^{a-1}) .$$

Separate the two cases when a is odd and when a is even. Suppose a is odd. Then l must be odd too, as $B_1(v_i, v_ix^k) = 0 = B_2(u_i, u_iy^k)$ for any even integer k with $0 \le k < a-1$ (see Definition 3.3.3). Notice that in this case $a \ge l+2 \ge 3$ so $\mathbf{F}_{q^2}$ must be a field of odd characteristic. Since l is an odd number,

$$x^l + \tau(x)^l = x^l + (\sum_{k=1}^{a-1}(-1)^kx^k)^l$$

is a polynomial of x of degree at least $l+1$ with integer coefficients, therefore

$$B_1(v_i, v_i[x^l + \tau(x)^l]) = B_2(u_i, u_i[y^l + \tau(y)^l]) .$$

And since $B_1(v_i, v_i x^l), B_2(u_i, u_i x^l) \in \mathbf{F}_q$ (also by the definition of standard bases),

$$\begin{aligned}
B_1(v_i, v_i x^l) &= \frac{1}{2}(B_1(v_i, v_i x^l) + \overline{B_1(v_i, v_i x^l)}) \\
&= \frac{1}{2}(B_1(v_i, v_i x^l) + B_1(v_i x^l, v_i)) \\
&= \frac{1}{2}(B_1(v_i, v_i x^l) + B_1(v_i, v_i \tau(x)^l)) \\
&= \frac{1}{2}B_1(v_i, v_i[x^l + \tau(x)^l]) \\
&= \frac{1}{2}B_2(u_i, u_i[y^l + \tau(y)^l]) \\
&= \frac{1}{2}(B_2(u_i, u_i y^l) + B_2(u_i, u_i \tau(y)^l)) \\
&= \frac{1}{2}(B_2(u_i, u_i y^l) + B_2(u_i y^l, u_i)) \\
&= \frac{1}{2}(B_2(u_i, u_i y^l) + \overline{B_2(u_i, u_i y^l)}) \\
&= B_2(u_i, u_i y^l) \; ,
\end{aligned}$$

a contradiction. Suppose a is even. Then l must be even also, as $B_1(v_i, v_i x^k) = 0 = B_2(u_i, u_i y^k)$ for any odd integer k with $0 \leq k < a - 1$. If the characteristic is 2 then $a = 2$, $l = 0$ and $B_1(v_i, v_i) = 0 = B_2(u_i, u_i)$, so from now on, we may assume that the characteristic is odd. Since l is even

$$x^l - \tau(x)^l = x^l - (\sum_{k=1}^{a-1}(-1)^k x^k)^l$$

is a polynomial of x of degree at least $l + 1$ with integer coefficients, therefore

$$B_1(v_i, v_i[x^l - \tau(x)^l]) = B_2(u_i, u_i[y^l - \tau(y)^l]) \; .$$

And since $B_1(v_i, v_ix^l), B_2(u_i, u_ix^l) \in \delta\mathbf{F}_q$ (by the definition of standard bases),

$$\begin{aligned}
B_1(v_i, v_ix^l) &= \frac{1}{2}(B_1(v_i, v_ix^l) - \overline{B_1(v_i, v_ix^l)}) \\
&= \frac{1}{2}(B_1(v_i, v_ix^l) - B_1(v_ix^l, v_i)) \\
&= \frac{1}{2}(B_1(v_i, v_ix^l) - B_1(v_i, v_i\tau(x)^l)) \\
&= \frac{1}{2}B_1(v_i, v_i[x^l - \tau(x)^l]) \\
&= \frac{1}{2}B_2(u_i, u_i[y^l - \tau(y)^l]) \\
&= \frac{1}{2}(B_2(u_i, u_iy^l) - B_2(u_i, u_i\tau(y)^l)) \\
&= \frac{1}{2}(B_2(u_i, u_iy^l) - B_2(u_iy^l, u_i)) \\
&= \frac{1}{2}(B_2(u_i, u_iy^l) - \overline{B_2(u_i, u_iy^l)}) \\
&= B_2(u_i, u_iy^l) ,
\end{aligned}$$

a contradiction. This completes the proof. ■

Theorem 3.3.8 *Let $g, h \in I(V, B)$ homogeneous elements of order p, $x = g - 1$, $y = h - 1$, and assume that $\dim_{\mathbf{F}_{q^2}} \ker(x) = \dim_{\mathbf{F}_{q^2}} \ker(y) = b$. Then g and h are conjugate in $I(V, B)$.*

Proof: Let $\beta_g = \{v_ix^k \,|\, 1 \le i \le b,\, 0 \le k \le a-1\}$ and $\beta_h = \{u_iy^k \,|\, 1 \le i \le b,\, 0 \le k \le a-1\}$ be standard bases for (V, B, g) and (V, B, h), respectively. Define the linear transformation $z \in \mathrm{GL}(V)$ by

$$v_ix^kz = u_iy^k \quad (1 \le i \le b,\, 0 \le k \le a-1)$$

so obviously $h = z^{-1}gz$ and $y = z^{-1}xz$ and by Lemma 3.3.7 $z \in I(V, B)$. ■

Theorem 3.3.9

$$|C_{I(V,B)}(g)| = q^{ab^2} \cdot \prod_{k=1}^{b} \left(1 - \frac{(-1)^k}{q^k}\right) .$$

Proof: According to Lemma 3.3.7 if $\{v_i \mid 1 \leq i \leq b\}$ and $\{u_i \mid 1 \leq i \leq b\}$ are ordered subsets of V such that

$$\beta_1 = \{v_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

and

$$\beta_2 = \{u_i x^k \mid 1 \leq i \leq b, 0 \leq k \leq a-1\}$$

are standard bases for (V, B, g) then there is an element z in $C_{I(V,B)}(g)$, the centralizer of g in $I(V, B)$, such that $v_i x^k z = u_i x^k$ for all i and k. In other words, $C_{I(V,B)}(g)$ acts transitively (and thus regularly) on the standard bases of (V, B, g). This means that the order of $C_{I(V,B)}(g)$ is equal to the number of standard bases for (V, B, g), which number is calculated in Lemma 3.3.6. ■

3.4 Arbitrary Elements of Order p in GL, Sp and GU Groups

Throughout this section V is a vector space over a field $\mathbf{F}$ of characteristic p, $B : V \times V \to \mathbf{F}$ is a bilinear or sesquilinear form on V, g is an element of order p in the isometry group $I(V, B)$ of (V, B) and we assume that one of the following holds.

1. $B \equiv 0$ and $\mathbf{F} = \mathbf{F}_q$ with $q = p^f$,
2. B is a non-singular symplectic form on V, $\mathbf{F} = \mathbf{F}_q$ with $q = p^f$ and p is an odd prime,
3. B is a non-singular unitary form on V and $\mathbf{F} = \mathbf{F}_{q^2}$ with $q = p^{2f}$.

Notation: For any pair (a, b) of positive integers with $a \leq p$, let $V_{a,1}$ be the quotient module of the regular $\mathbf{F}\langle g\rangle$-module having dimension a over bfF, and let $V_{a,b}$ be the direct sum of b copies of $V_{a,1}$.

The $\mathbf{F}\langle g\rangle$-module V decomposes into a direct sum of homogeneous $\mathbf{F}\langle g\rangle$-modules, say

$$V = \bigoplus_{i=1}^{e} V_i\,, \quad V_i \simeq V_{a_i,b_i} \tag{3.1}$$

where $1 \leq a_i < a_j \leq p$ for all $1 \leq i < j \leq e$. Of course, $e \leq p$ and $\sum_{i=1}^{e} a_i b_i = d$. According to the well-known Krull-Schmidt Theorem, the numbers e, a_i, b_i $(1 \leq i \leq e)$ are uniquely determined by V. However, the decomposition in (3.1) itself is not unique in general. Most of this section will be devoted to studying these decompositions of V into a direct sum of homogeneous submodules.

We say that such a decomposition $V = \bigoplus_{i=1}^{e} V_i$ is **orthogonal** is $B(v_i, v_j) = 0$ whenever $v_i \in V_i$, $v_j \in V_j$ and $i \neq j$.

Lemma 3.4.1 *Suppose B is a non-singular form on V then for any non-negative integer a,*

$$Vx^a = \ker(x^a)^{\perp}\,.$$

Proof: Using the fact that $\tau(x) = -x(1+x)^{-1}$, if $v \in V$ and $u \in \ker(x^a)$ then

$$B(vx^a, u) = B(v, u\tau(x)^a) = (-1)^a B(v, ux^a(1+x)^{-a}) = 0\,.$$

This shows that $Vx^a \subseteq \ker(x^a)^{\perp}$. And equality holds since

$$\dim Vx^a = d - \dim\ker(x^a) = \dim\ker(x^a)^{\perp}\,. \quad \blacksquare$$

Lemma 3.4.2 *Let $V = \bigoplus_{i=1}^{e} V_i$ as in (3.1) and assume that B is a non-singular form on V. Then the restriction of B to V_1 is also non-singular.*

Proof: Suppose $0 \neq v \in V_1 \cap \ker(x)$. Let

$$W_1 = \ker(x^{a_1}) \cap \Big(\bigoplus_{i=2}^{e} V_i\Big)$$

so

$$\ker(x^{a_1}) = V_1 \oplus W_1\,.$$

Since $W_1 \subseteq Vx$ and $v \in \ker(x)$, by Lemma 3.4.1 v is perpendicular to W_1. But also by the same lemma, v is not perpendicular to $V_1 \oplus W_1$ since $v \notin Vx^a = \ker(x^a)^\perp$. Hence v is not perpendicular to V_1.

Now suppose v is any non-zero vector in V_1. There is a non-negative integer k such that $vx^k \neq 0$ and $vx^{k+1} = 0$. Then by the above argument, $B(v, u\tau(x)^k) = B(vx^k, u) \neq 0$ for some $u \in V_1$. ■

Lemma 3.4.3 *If $V \simeq V_{a,b}$ and a_1 is a positive integer different from a then*

$$Vx^{a_1-1} \cap \ker(x) \subseteq Vx^{a_1} .$$

Proof: If $a_1 > a$ then $Vx^{a_1-1} = \{0\}$. And if $a_1 < a$ then $\ker(x) \subseteq Vx^{a-1} \subseteq Vx^{a_1}$. ■

Lemma 3.4.4 *Let $V = \bigoplus_{i=1}^{e} V_i = \bigoplus_{i=1}^{e} U_i$ be two decompositions of V into direct sums of homogeneous $\mathbf{F}\langle g\rangle$-modules with $V_i \simeq U_i \simeq V_{a_i,b_i}$ $(1 \le i \le i)$ and $1 \le a_i < a_j \le p$ for $1 \le i < j \le e$, as usual. Let $1 \le k \le e$ and let $\pi_k : V \to V_k$ be the projection map of V onto V_k with $\ker(\pi_i) = \bigoplus_{i \neq k} V_i$. Then*

$$U_k\pi_k = V_k .$$

Proof: By way of contradiction, suppose that $U_k\pi_k \subsetneqq V_k$ and thus there is a non-zero vector u in U_k such that $u\pi_k = 0$. This means that $u \in \bigoplus_{i \neq k} V_i$. Since both U_k and $\bigoplus_{i \neq k} V_i$ are $\mathbf{F}\langle g\rangle$-submodules of V, we may assume that

$$u \in U_k \cap \bigoplus_{i \neq k} V_i \cap \ker(x) .$$

Now $u \in U_k \cap \ker(x)$ implies that $u \in Vx^{a_k-1}$. Furthermore, since $u \in Vx^{a_k-1}$ and $u \in \bigoplus_{i \neq k} V_i$, it follows from Lemma 3.4.3 that $u \in Vx^{a_k}$. This is a contradiction as $Vx^{a_k} \cap U_k = \{0\}$. ■

Lemma 3.4.5 *Let* $V = \bigoplus_{i=1}^{e} V_i$ *as in (3.1) and let* U_i $(1 \leq i \leq e)$ *be direct summands of* V *such that* $U_i \simeq V_i$ *for all* i. *Then* $V = \bigoplus_{i=1}^{e} U_i$.

Proof: Let π_1 be the projection map of V onto V_1 with $\ker(\pi_1) = \bigoplus_{i=2}^{e} V_i$. Then according to the previous lemma, $U_1\pi_1 = V_1$ and thus

$$V = U_1 \oplus \big(\bigoplus_{i=2}^{e} V_i\big)$$

By repeating the same argument, one can easily use an induction to show that

$$V = \big(\bigoplus_{i=1}^{k} U_i\big) \oplus \big(\bigoplus_{i=k+1}^{e} V_i\big)$$

for any $0 \leq k \leq e$. ■

Lemma 3.4.6 *If* a_i, b_i $(i = 1, 2)$ *are positive integers such that* $a_1, a_2 \leq p$, *and* $a = \min\{a_1, a_2\}$ *then*

$$|\, Hom_{\mathbf{F}\langle g\rangle}(V_{a_1,b_1}, V_{a_2,b_2})\,| = |\mathbf{F}|^{ab_1b_2}\ .$$

Proof: Let $\bar{\beta} = \{v_1, v_2, \dots, v_{b_1}\}$ be an ordered subset of V_{a_1,b_1} such that $\beta = \{v_i x^k \,|\, 1 \leq i \leq b_1, 0 \leq k \leq a_1\}$ is a basis for V_{a_1,b_1} over $\mathbf{F}$. Then for any $\varphi \in \mathrm{Hom}_{\mathbf{F}\langle g\rangle}(V_{a_1,b_1}, v_{a_2,b_2})$, the set $\bar{\beta}\varphi = \{v_i\varphi \,|\, 1 \leq i \leq b_1\}$ is a subset of $V_{a_2,b_2} \cap \ker(x^{a_1})$. On the other hand, if $u_1, u_2, \dots, u_{b_1}$ are any vectors in $V_{a_2,b_2} \cap \ker(x^{a_1})$, then there is a unique homomorphism φ from V_{a_1,b_1} to V_{a_2,b_2} such that $v_i\varphi = u_i$ for all i. Therefore,

$$|\, \mathrm{Hom}_{\mathbf{F}\langle g\rangle}(V_{a_1,b_1}, v_{a_2,b_2})\,| = |\, V_{a_2,b_2} \cap \ker(x^{a_1})\,|^{b_1} = |\mathbf{F}|^{ab_1b_2}\ ,$$

as stated. ■

Lemma 3.4.7 *Let* $V = \bigoplus_{i=1}^{e} V_i$ *as in (3.1) and let* $1 \leq k \leq e$. *Then the number of direct summands of* V *isomorphic to* V_k *is*

$$\prod_{\substack{1 \leq i \leq e \\ i \neq k}} |\mathbf{F}|^{\min\{a_i, a_k\} b_i b_k}\ .$$

Proof: Let $W_k = \bigoplus_{i \neq k} V_i$ and let π_k be the projection map of V onto V_k with $\ker(\pi_k) = W_k$. So if U is a direct summand of V isomorphic to V_k then by Lemma 3.4.4 the restriction of π_k to U gives an isomorphism from U to V_k. It follows from this fact that there is a map $\alpha : V_k \to W_k$ such that

$$U = \{v + v\alpha \,|\, v \in V_k\} \,.$$

It is easy to see that actually α must be an $\mathbf{F}\langle g \rangle$-module homomorphism. For if $v_1, v_2 \in V$ then

$$(v_1 + v_1\alpha) + (v_2 + v_2\alpha) \text{ and } (v_1 + v_2) + (v_1 + v_2)\alpha$$

are both elements of U that map to $v_1 + v_2$ under π_k, hence they are equal, which means that

$$v_1\alpha + v_2\alpha = (v_1 + v_2)\alpha \,,$$

and this is true for any two vectors v_1 and v_2 in V_k. Also, if $v \in V_k$ then $vg \in V_k$ so $(v + v\alpha)g$ and $vg + (vg)\alpha$ are both elements of U that project to vg under the map π_k. Hence $(v + v\alpha)g = vg + (vg)\alpha$ and $v\alpha g = (vg)\alpha$.

On the other hand if α is any $\mathbf{F}\langle g \rangle$-module homomorphism from V_k to W_k then it is easy to check that the set $U = \{v + v\alpha \,|\, v \in V_k\}$ is an $\mathbf{F}\langle g \rangle$-submodule of V that maps isomorphically to V_k under the projection π_k. Furthermore, $V = U \oplus \bigoplus_{i \neq k} V_i$, so U is a direct summand of V.

This shows that there is a one-to-one correspondence between the elements of $\mathrm{Hom}_{\mathbf{F}\langle g \rangle}(V_k, W_k)$ and the direct summands of V that are isomorphic to V_k. And by Lemma 3.4.6

$$|\,\mathrm{Hom}_{\mathbf{F}\langle g \rangle}(V_k, W_k)\,| = \prod_{\substack{1 \leq i \leq e \\ i \neq k}} |\mathbf{F}|^{\min\{a_i, a_k\} b_i b_k} \,. \quad \blacksquare$$

Lemma 3.4.8 *Let* $V = \bigoplus_{i=1}^{e} V_i$ *as in (3.1). Then the number of such decompositions of* V *into a direct sum of homogeneous* $\mathbf{F}\langle g\rangle$*-modules is*

$$\prod_{1\le i<j\le e} |\mathbf{F}|^{2a_ib_ib_j} = |\mathbf{F}|^{2\sum\limits_{1\le i<j\le e} a_ib_ib_j} .$$

Proof: Follows immediately from Lemmas 3.4.5 and 3.4.7. ■

Lemma 3.4.9 *Let* $V = \bigoplus_{i=1}^{e} V_i$ *as in (3.1) and assume that* B *is a non-singular form on* V*. Then the number of orthogonal decompositions of* V *into a direct sum of homogeneous* $\mathbf{F}\langle g\rangle$*-modules is*

$$\prod_{1\le i<j\le e} |\mathbf{F}|^{a_ib_ib_j} = |\mathbf{F}|^{\sum\limits_{1\le i<j\le e} a_ib_ib_j} .$$

Proof: By induction on e. If $e = 1$ then there is nothing to prove. If $e > 1$ and U_1 is any direct summand of V that is isomorphic to V_1, then by Lemma 3.4.2 $V = U_1 \oplus U_1^{\perp}$, therefore $U_1^{\perp} \simeq \bigoplus_{i=2}^{e} V_i$ as $\mathbf{F}\langle g\rangle$-modules; and by the induction hypothesis the number of orthogonal decompositions of $U_1^{\perp}$ into a direct sum of homogeneous $\mathbf{F}\langle g\rangle$-modules is

$$\prod_{2\le i<j\le e} |\mathbf{F}|^{a_ib_ib_j} .$$

By Lemma 3.4.7 the number of choices for U_1 is

$$\prod_{i=2}^{e} |\mathbf{F}|^{a_1b_1b_i} ,$$

the statement of the lemma follows immediately. ■

Lemma 3.4.10 *Suppose* B *is a non-singular form on* V*. Then* $C_{I(V,B)}(g)$ *acts transitively on the orthogonal decompositions of* V*.*

Proof: Let $V = \bigoplus_{i=1}^{e} V_i = \bigoplus_{i=1}^{e} U_i$ be two orthogonal decompositions of V with $V_i \simeq U_i \simeq V_{a_i,b_i}$ for all $1 \le i \le e$ and $1 \le a_i < a_j \le p$ for all $1 \le i < j \le e$. It is sufficient to show that for each k there is an $\mathbf{F}\langle g\rangle$-module isomorphism $z_k : V_k \to U_k$ that is also an isometry between (V_k, B) and (U_k, B). According to Lemmas 3.2.12 and 3.3.7 the existence of such a map z_k is guaranteed if there is an isometry between the induced forms $\overline{B}_1$ and $\overline{B}_2$ on $W_1 = V_k \cap \ker(x)$ and $W_2 = U_k \cap \ker(x)$, respectively (as described in Definitions 3.2.3 and 3.3.1). In other words, it is enough to construct a map $\varphi_k : W_1 \to W_2$ with the property that for any $v_1, v_2 \in V_k$ there are vectors $u_1, u_2 \in U_k$ such that

$$\begin{aligned} v_1 x^{a_k-1}\varphi_k &= u_1 x^{a_k-1} , \\ v_2 x^{a_k-1}\varphi_k &= u_2 x^{a_k-1} , \\ B(v_1, v_2 x^{a_k-1}) &= B(u_1, u_2 x^{a_k-1}) . \end{aligned}$$

As we saw it in the proof of Lemma 3.4.7, there is an $\mathbf{F}\langle g\rangle$-module homomorphism $\alpha : V_k \to V_k^\perp = \bigoplus_{i\neq k} V_i$ such that $U_k = \{v + v\alpha \,|\, v \in V_k\}$, and the map $v \mapsto v + v\alpha$ is an isomorphism from V_k to U_k. Define φ_k to be the restriction of this map to $W_1 = V_k \cap \ker(x)$. Then for any $v_1, v_2 \in V_k$, let $u_1 = v_1 + v_1\alpha$, $u_2 = v_2 + v_2\alpha$, so

$$\begin{aligned} u_1 x^{a_k-1} &= (v_1 + v_1\alpha)x^{a_k-1} \\ &= v_1 x^{a_k-1} + v_1 x^{a_k-1}\alpha \\ &= v_1 x^{a_k-1}\varphi_k , \\ u_2 x^{a_k-1} &= (v_2 + v_2\alpha)x^{a_k-1} \\ &= v_2 x^{a_k-1} + v_2 x^{a_k-1}\alpha \\ &= v_2 x^{a_k-1}\varphi_k , \\ B(u_1, u_2 x^{a_k-1}) &= B(v_1 + v_1\alpha, (v_2 + v_2\alpha)x^{a_k-1}) \\ &= B(v_1, v_2 x^{a_k-1}) + B(v_1\alpha, v_2 x^{a_k-1}) + \\ &\quad + B(v_1 + v_1\alpha, v_2\alpha x^{a_k-1}) . \end{aligned}$$

Here, $v_2 x^{a_k-1} \in \ker(x)$, so $v_2 x^{a_k-1}\alpha \in \ker(x) \cap \bigoplus_{i\neq k} V_i$ and by Lemma 3.4.3 $v_2 x^{a_k-1}\alpha \in V x^{a_k}$. Then by Lemma 3.4.1 $v_2 x^{a_k-1}\alpha$ is perpendicular to $\ker(x^a)$, in particular

$$B(v_1 + v_1\alpha, v_2\alpha x^{a_k-1}) = B(v_1 + v_1\alpha, v_2 x^{a_k-1}\alpha) = 0 .$$

By a similar argument,

$$B(v_1\alpha, v_2x^{a_k-1}) = B(v_1\tau(x)^{a_k-1}\alpha, v_2) = 0$$

since $v_2 \in \ker(x^{a_k})$ and $v_1\tau(x)^{a_k-1}\alpha \in Vx^{a_k}$. Hence

$$B(u_1, u_2x^{a_k-1}) = B(v_1, v_2x^{a_k-1})$$

as wanted. This completes the proof. ■

Theorem 3.4.11 *Assume V is a vector space of dimension d over $\mathbf{F}_q$ ($q = p^f$), $g \in GL(V)$ is an element of order p and*

$$V \simeq \bigoplus_{i=1}^{e} V_{a_i,b_i}$$

as $\mathbf{F}_q\langle g\rangle$-modules with $1 \leq a_i < a_j \leq p$ for all $1 \leq i < j \leq e$. Then

$$|C_{\mathrm{GL}(V)}(g)| = q^{\sum_{i=1}^{e}\sum_{j=1}^{e} \min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e}\prod_{k=1}^{b_i}\left(1-\frac{1}{q^k}\right).$$

Proof: By Lemma 3.4.8 the number of decompositions of V into a direct sum of homogeneous $\mathbf{F}_q\langle g\rangle$-submodules is

$$\prod_{1\leq i<j\leq e} q^{2a_ib_ib_j} = q^{2\sum_{1\leq i<j\leq e} a_ib_ib_j}.$$

And because any two such decompositions of V are the same up to isomorphism, it is easy to see that $C_{\mathrm{GL}(V)}(g)$ acts transitively on these decompositions. Since the order of the stabilizer of one decomposition is

$$\prod_{i=1}^{e} |C_{I(V_{a_i,b_i},B)}(g)|$$

and since

$$|C_{I(V_{a_i,b_i},B)}(g)| = q^{a_ib_i^2}\prod_{k=1}^{b_i}\left(1-\frac{1}{q^k}\right)$$

for all i by Theorem 3.1.3,

$$\begin{aligned} |C_{\mathrm{GL}(V)}(g)| &= q^{2\sum_{1\leq i<j\leq e} a_i b_i b_j} \prod_{i=1}^{e} \left[q^{a_i b_i^2} \prod_{k=1}^{b_i} \left(1 - \frac{1}{q^k}\right) \right] \\ &= q^{\sum_{i=1}^{e}\sum_{j=1}^{e} \min\{a_i,a_j\} b_i b_j} \prod_{i=1}^{e} \prod_{k=1}^{b_i} \left(1 - \frac{1}{q^k}\right) \end{aligned}$$

as stated. ∎

Theorem 3.4.12 *Assume that V is a vector space of dimension d over $\mathbf{F}_{q^2}$, B is a non-singular unitary form on V, $g \in I(V,B)$ is an element of order p and*

$$V \simeq \bigoplus_{i=1}^{e} V_{a_i,b_i}$$

as $\mathbf{F}_{q^2}\langle g\rangle$-modules with $1 \leq a_i < a_j \leq p$ for all $1 \leq i < j \leq e$. Then

$$|C_{I(V,B)}(g)| = q^{\sum_{i=1}^{e}\sum_{j=1}^{e} \min\{a_i,a_j\} b_i b_j} \prod_{i=1}^{e} \prod_{k=1}^{b_i} \left(1 - \frac{(-1)^k}{q^k}\right).$$

Proof: By Lemma 3.4.9 the number of orthogonal decompositions of V into a direct sum of homogeneous $\mathbf{F}_{q^2}\langle g\rangle$-submodules is

$$\prod_{1\leq i<j\leq e} |\mathbf{F}_{q^2}|^{a_i b_i b_j} = q^{2\sum_{1\leq i<j\leq e} a_i b_i b_j}.$$

And by Lemma 3.4.10, $C_{I(V,B)}(g)$ acts transitively on these decompositions. Since the order of the stabilizer of one orthogonal decomposition is

$$\prod_{i=1}^{e} |C_{I(V_{a_i,b_i},B)}(g)|$$

and since

$$|C_{I(V_{a_i,b_i},B)}(g)| = q^{a_i b_i^2} \prod_{k=1}^{b_i} \left(1 - \frac{(-1)^k}{q^k}\right)$$

by Theorem 3.3.9,

$$\begin{aligned} |C_{I(V,B)}(g)| &= q^{2\sum_{1\leq i<j\leq e} a_i b_i b_j} \prod_{i=1}^{e} \left[q^{a_i b_i^2} \prod_{k=1}^{b_i} \left(1 - \frac{(-1)^k}{q^k}\right) \right] \\ &= q^{\sum_{i=1}^{e}\sum_{j=1}^{e} \min\{a_i,a_j\} b_i b_j} \prod_{i=1}^{e} \prod_{k=1}^{b_i} \left(1 - \frac{(-1)^k}{q^k}\right) \end{aligned}$$

as stated. ∎

Theorem 3.4.13 *Assume that V is a vector space of dimension d over $\mathbf{F}_q$ (q an odd prime power), B is a non-singular symplectic form on V, $g \in I(V,B)$ is an element of order p and*

$$V = \bigoplus_{i=1}^{e} V_i$$

as $\mathbf{F}_q\langle g\rangle$-modules with $V_i \simeq V_{a_i,b_i}$ for all i and $1 \leq a_i < a_j \leq p$ for all $1 \leq i < j \leq e$. Then

$$|C_{I(V,B)}(g)| = q^{\frac{1}{2}\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e} \prod_{\substack{1\leq k\leq b_i \\ k \text{ even}}} \left(1 - \frac{1}{q^k}\right) \cdot \rho(V_i, B, g)\,.$$

Proof: The proof follows exactly the same line of reasoning as the proof for the previous theorem, with the only difference that this time we refer to Theorem 3.2.16.

■

3.5 Centralizer Orders of p'-Elements in GL, Sp and GU Groups

Notation. Throughout this section we will use the following notations. V is a vector space of dimension d over a field $\mathbf{F}$ of characteristic p, B is a non-singular symplectic or unitary form on V, τ is the anti-isomorphism of $\mathrm{End}_{\mathbf{F}}(V)$ with the property that

$$B(u\varphi, v) = B(u, v\tau(\varphi))$$

for all $u, v \in V$ and $\varphi \in \mathrm{End}_{\mathbf{F}}(V)$. $I(V,B)$ is the isometry group of (V,B) and g is an element of $\mathrm{GL}(V)$ with $|g| = o$ and $\gcd(o,p) = 1$. Unless otherwise stated, we always assume that $g \in I(V,B)$. In the case if B is symplectic, let $\mathbf{F} = \mathbf{F}_q$ and if B is a unitary form, let $\mathbf{F} = \mathbf{F}_{q^2}$, ($q = p^f$ for some prime p). The polynomial $x^o - 1$ decomposes into a product of irreducible polynomials over $\mathbf{F}$:

$$x^o - 1 = \prod_{i=1}^{t} f_i(x)$$

and $f_i \neq f_j$ for $i \neq j$ since $x^o - 1$ does not have multiple roots. For each $1 \leq i \leq t$, let m_i be the degree of f_i, and let i' be the unique number between 1 and t such that $f_{i'}(x)$ is a constant multiple of $x^{m_i}\bar{f}(x^{-1})$. Let I denote the set of numbers i with $i' = i$ and let $J = \{1 \leq i \leq t \,|\, i' \neq i\}$. Furthermore, let $I_1 = \{i \in I \,|\, f_i(x) = x - 1 \text{ or } f_i(x) = x + 1\}$ and let $I_2 = I \backslash I_1$. Also for each $1 \leq i \leq t$ let

$$V_i = \{v \in V \,|\, v f_i(g) = 0\} \,,$$

let d_i be the dimension of V_i over $\mathbf{F}$, n_i be the number of direct summands in a decomposition of V_i into a direct sum of irreducible $\mathbf{F}\langle g\rangle$-modules, and let F_i be the the center of the automorphism-group of the $\mathbf{F}\langle g\rangle$-module V_i, together with the 0 map. That is, $F_i = Z\Big(\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)\Big) \cup \{0\}$. Then we have the following:

$$\begin{aligned}
V &= V_1 \oplus V_2 \oplus \ldots \oplus V_t \,, \\
d &= \sum_{i=1}^{t} d_i \,, \\
d_i &= m_i \cdot n_i \quad (\text{for all } 1 \leq i \leq t)\,, \\
F_i &\simeq \mathbf{F}_{q^{\varepsilon m_i}} \,, \\
\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i) &\simeq \mathrm{GL}_{n_i}(q^{\varepsilon m_i}) \,, \\
C_{\mathrm{GL}(V)}(g) &\simeq \prod_{i=1}^{t} \mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i) \\
&\simeq \prod_{i=1}^{t} \mathrm{GL}_{n_i}(q^{\varepsilon m_i}) \,,
\end{aligned}$$

where

$$\varepsilon = \begin{cases} 1, & \text{if } B \text{ is symplectic;} \\ 2, & \text{if } B \text{ is unitary.} \end{cases}$$

Notice that these formulas do not require g to be in in $I(V, B)$. Finally, for each $1 \leq i \leq t$ let π_i be the projection map of V onto V_i with $\ker(\pi_i) = \bigoplus_{j\neq i} V_j$, and let κ_i be the natural embedding of $\mathrm{End}_{\mathbf{F}}(V_i)$ into $\mathrm{End}_{\mathbf{F}}(V)$, so that for any $\varphi \in \mathrm{End}_{\mathbf{F}}(V_i)$,

$$v\kappa_i(\varphi) = \begin{cases} v\varphi, & \text{if } v \in V_i \,; \\ 0, & \text{if } v \in \bigoplus_{j\neq i} V_j \,. \end{cases}$$

In particular, $\kappa_i(1_{V_i}) = \pi_i$.

Lemma 3.5.1 *For any* $1 \leq i \leq t$, $V_i^{\perp} = \bigoplus_{j \neq i'} V_j$. *That is,* $V_i \perp V_j$ *for all* i *and* j *unless* $j = i'$.

Proof: If $v \in V_i$ then for all $w \in V$

$$0 = B(0, w) = B(vf_i(g), w) = B(v, w\tau(f_i(g))) =$$

$$= B(v, w\bar{f}_i(\tau(g))) = B(v, w\bar{f}_i(g^{-1}))$$

and so $0 = B(v, wf_{i'}(g))$. This shows that $Vf_{i'}(g) = \bigoplus_{j \neq i'} V_j$ is contained in $V_i^{\perp}$. In particular, $\dim_{\mathbf{F}} V_i + \sum_{j \neq i'} \dim_{\mathbf{F}} V_j \leq \dim_{\mathbf{F}} V_i + \dim_{\mathbf{F}}(V_i)^{\perp} \leq \dim_{\mathbf{F}} V$, which means that $\dim_{\mathbf{F}} V_i \leq \dim_{\mathbf{F}} V_{i'}$. But obviously a similar argument can be used to show that $\dim_{\mathbf{F}} V_{i'} \leq \dim_{\mathbf{F}} V_i$, hence V_i and $V_{i'}$ have the same dimension over **F**. Then this implies that the inclusion of $\bigoplus_{j \neq i'} V_j$ in $V_i^{\perp}$ can not be a strict inclusion, because their dimension over **F** is the same. ∎

Corollary 3.5.2 *For each* i, $d_i = d_{i'}$ *and* $n_i = n_{i'}$.

Lemma 3.5.3 *If* $\varphi \in C_{GL(V)}(g)$ *then* $V_i\varphi = V_i$ *for all* i.

Proof: For all $1 \leq i \leq t$ and $v \in V_i$, $v\varphi f_i(g) = v f_i(g)\varphi = 0\varphi = 0$, hence $V_1\varphi \leq V_1$. And equality holds because φ is non-singular. ∎

Lemma 3.5.4 *Let* $\varphi \in End_{\mathbf{F}}(V)$.

- *If* $V\varphi \leq V_i$ *then* $\bigoplus_{j \neq i'} V_j \leq \ker(\tau(\varphi))$.
- *If* $V\varphi = V_i$ *then* $\bigoplus_{j \neq i'} V_j = \ker(\tau(\varphi))$.
- *If* $\bigoplus_{j \neq i} V_j \leq \ker(\varphi)$ *then* $V\tau(\varphi) \leq V_{i'}$.
- *If* $\bigoplus_{j \neq i} V_j = \ker(\varphi)$ *then* $V\tau(\varphi) = V_{i'}$.

Proof: If $V\varphi \leq V_i$ then $\bigoplus_{j\neq i'} V_j = V_i^{\perp} \leq (V\varphi)^{\perp}$, so $v \in \bigoplus_{j\neq i'} V_j$ implies that $B(w, v\tau(\varphi)) = B(w\varphi, v) = 0$ for all $w \in V$. That is, $v \in \ker(\tau(\varphi))$. This shows that $\bigoplus_{j\neq i'} V_j \leq \ker(\tau(\varphi))$.

If $V\varphi = V_i$ then by the above argument $\bigoplus_{j\neq i'} V_j \leq \ker(\tau(\varphi))$ and equality must hold because

$$\dim \bigoplus_{j\neq i'} V_j = d - \dim V_{i'} = d - \dim V_i =$$

$$= d - \dim V\varphi_i = \dim \ker(\varphi_i) = \dim \ker(\tau(\varphi_i)) \ .$$

If $\bigoplus_{j\neq i} V_j \leq \ker(\varphi)$ then for all $v \in V$ and $w \in \bigoplus_{j\neq i} V_j$, $B(v\tau(\varphi), w) = B(v, w\varphi) = B(v, 0) = 0$, so $v\tau(\varphi) \in \left(\bigoplus_{j\neq i} V_j\right)^{\perp} = V_{i'}$. That is, $V\tau(\varphi) \leq V_{i'}$.

If $\bigoplus_{j\neq i} V_j = \ker(\varphi)$ then by the above argument $V\tau(\varphi) \leq V_{i'}$ and equality must hold because

$$\dim V\tau(\varphi) = \dim V\varphi = d - \dim \ker(\varphi) =$$

$$d - \dim \bigoplus_{j\neq i} V_j = \dim V_i = \dim V_{i'} \ .$$

This completes the proof. ■

Lemma 3.5.5 *For each* $1 \leq i \leq t$, $\tau(\pi_i) = \pi_{i'}$.

Proof: First, $\tau(\pi_i)\tau(\pi_i) = \tau(\pi_i^2) = \tau(\pi_i)$ so $\tau(\pi_i)$ is a projection. Then from the previous lemma, $\ker(\tau(\pi_i)) = \bigoplus_{j\neq i'} V_j$ and $V\tau(\pi_i) = V_{i'}$, so $\tau(\pi_i) = \pi_{i'}$. ■

Definition 3.5.6 *For each* $1 \leq i \leq t$ *define a map*

$$\tau_i : End_{\mathbf{F}}(V_i) \to End_{\mathbf{F}}(V_{i'})$$

as follows. Suppose $\varphi \in End_{\mathbf{F}}(V_i)$. *Then* $\kappa_i(\varphi) \in End_{\mathbf{F}}(V)$ *as described in the beginning of this section and by Lemma 3.5.4,* $\bigoplus_{j\neq i'} V_j \leq \ker(\tau(\kappa_i(\varphi)))$ *and* $V\tau(\kappa_i(\varphi)) \leq$

$V_{i'}$. Therefore, $\tau(\kappa_i(\varphi)) \in \kappa_{i'}(End_{\mathbf{F}}(V_{i'}))$ and we define $\tau_i(\varphi)$ to be the unique element of $End_{\mathbf{F}}(V_{i'})$ with the property that

$$\tau(\kappa_i(\varphi)) = \kappa_{i'}(\tau_i(\varphi)) \ .$$

It is easy to see that τ_i is an algebra anti-isomorphism from $End_{\mathbf{F}}(V_i)$ to $End_{\mathbf{F}}(V_{i'})$.

Lemma 3.5.7 *If $\varphi \in End_{\mathbf{F}}(V)$ and*

$$\varphi = \bigoplus_{i=1}^{t} \varphi_i$$

where $\varphi_i \in End_{\mathbf{F}}(V_i)$ for all i then

$$\tau(\varphi) = \bigoplus_{i=1}^{t} \tau_i(\varphi_i) \ .$$

Proof: $\varphi = \bigoplus_{i=1}^{t} \varphi_i$ means that $\varphi = \sum_{i=1}^{t} \kappa_i(\varphi_i)$, therefore

$$\begin{aligned} \tau(\varphi) &= \sum_{i=1}^{t} \tau(\kappa_i(\varphi_i)) \\ &= \sum_{i=1}^{t} \kappa_{i'}(\tau_i(\varphi_i)) \\ &= \bigoplus_{i=1}^{t} \tau_i(\varphi_i) \end{aligned}$$

as stated. ∎

Lemma 3.5.8 *For each i, τ_i and $\tau_{i'}$ are inverses of each other.*

Proof: For any $\varphi \in \mathrm{End}_{\mathbf{F}}(V_i)$,

$$\begin{aligned} \kappa_{i'}(\tau_{i'}(\tau_i(\varphi))) &= \tau(\kappa_i(\tau_i(\varphi))) \\ &= \tau(\tau(\kappa_{i'}(\varphi))) \\ &= \kappa_{i'}(\varphi) \ , \end{aligned}$$

and therefore $\tau_{i'}(\tau_i(\varphi)) = \varphi$. This shows that $\tau_{i'}\tau_i = 1_{V_i}$, and a similar argument can be used to show that $\tau_i\tau_{i'} = 1_{V_{i'}}$. ∎

Lemma 3.5.9 *For each i, $\tau_i(F_i) = F_{i'}$.*

Proof: Recall that $F_i = C\Big(\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)\Big) \cup \{0\}$. It is easy to see that τ_i maps $\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)$ to $\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_{i'})$ (and the reason for this is simply that τ_i maps $\mathrm{End}_{\mathbf{F}\langle g\rangle}(V_i)$ to $\mathrm{End}_{\mathbf{F}\langle g\rangle}(V_{i'})$ and does not change the rank of a linear transformation). And the restriction of τ_i to $\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)$ is a bijective map, since we proved it in the previous lemma, that τ_i has an inverse. Hence τ_i must map the center of $\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)$ into the center of $\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_{i'})$. ■

Lemma 3.5.10 *If $i \in I$ then $\tau_i|_{F_i} \in Gal(F_i|\mathbf{F}_q)$. Furthermore, if $i \in I_1$ and B is a symplectic form then $\tau_i|_{F_i}$ is the identity element of $Gal(F_i|\mathbf{F}_q)$ and in any other case $\tau_i|_{F_i}$ is the unique involution of $Gal(F_i|\mathbf{F}_q)$.*

Proof: Recall that $\mathbf{F} = \mathbf{F}_q$ if B is a symplectic form, and $\mathbf{F} = \mathbf{F}_{q^2}$ if B is a unitary form. By Lemma 3.5.9 τ_i stabilizes F_i if $i \in I$. We also need to prove that inside F_i, τ_i fixes $\mathbf{F}_q$ elementwise. If $\alpha \in \mathbf{F}$, then $\tau(\alpha\varphi) = \alpha^q\tau(\varphi)$ for any $\varphi \in \mathrm{End}_{\mathbf{F}}(V)$, and

$$\tau_i(\alpha) = \tau_i(\alpha 1_{V_i}) = \kappa_{i'}^{-1}(\tau(\kappa_i(\alpha 1_{V_i}))) = \kappa_{i'}^{-1}(\tau(\alpha\kappa_i 1_{V_i})) =$$

$$= \kappa_{i'}^{-1}(\tau(\alpha\pi_i)) = \kappa_{i'}^{-1}(\alpha^q\pi_{i'}) = \alpha^q 1_{V_{i'}} .$$

This shows that the restriction of τ_i to F_i leaves $\mathbf{F}_q$ elementwise fixed in F_i whenever $i = i'$. And since τ_i is an algebra anti-isomorphism, its restriction to any cyclic group is a group-isomorphism, thus $\tau_i|_{F_i}$ is a field-automorphism of F_i.

According to Lemma 3.5.8, $\tau_i^2 = 1_{V_i}$, so $\tau_i|_{F_i}$ can be only either the identity element or an involution in $\mathrm{Gal}(F_i|\mathbf{F}_q)$. Since $g|_{V_i} \in F_i$, the first case would imply $\tau_i(g|_{V_i}) = g^{-1}|_{V_i} = g|_{V_i}$, that is $g^2 = 1$ on V_i, which means that $f_i(x)$ divides $x^2 - 1$ and therefore $i \in I_1$. This shows that $\tau_i|_{F_i}$ must be an involution (and therefore the unique involution) in $\mathrm{Gal}(F_i|\mathbf{F}_q)$ whenever $i \in I_2$. Also, if B is a unitary form and $\mathbf{F} = \mathbf{F}_{q^2}$, then as we saw above, τ_i acts as a conjugation on $\mathbf{F}$, so $\tau_i|_{F_i}$ can not be the identity element of $\mathrm{Gal}(F_i|\mathbf{F}_q)$.

On the other hand, if $i \in I_1$ and B is symplectic then $\mathrm{Aut}_{\mathbf{F}}(V_i) = \mathrm{GL}(V_i)$ and $F_i \simeq \mathbf{F}_q$, so actually the Galois group $\mathrm{Gal}(F_i|\mathbf{F}_q)$ is trivial. This completes the proof.

■

Definition 3.5.11 *For each $1 \leq i \leq t$ define a form B_i as follows:*

$$\begin{aligned} B_i : V_i \times V_{i'} &\longrightarrow F_i \\ (u,v) &\longmapsto \sum_{\lambda \in F_i^*} B(u\lambda^{-1}, v)\lambda \, . \end{aligned}$$

Also, let $Tr_i : F_i \to \mathbf{F}$ be the trace map:

$$Tr_i(\lambda) = \sum_{k=0}^{m_i - 1} \lambda^{q^k} \, .$$

Lemma 3.5.12 *For any $1 \leq i \leq t$ and $u \in V_i$, $v \in V_{i'}$,*

$$Tr_i(B_i(u,v)) = -B(u,v) \, .$$

Proof:

$$\begin{aligned} \mathrm{Tr}_i(B_i(u,v)) &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}, v)\mathrm{Tr}_i(\lambda) \\ &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}\mathrm{Tr}_i(\lambda), v) \\ &= B(u \sum_{\lambda \in F_i^*} \lambda^{-1}\mathrm{Tr}_i(\lambda), v) \end{aligned}$$

and

$$\begin{aligned} \sum_{\lambda \in F_i^*} \lambda^{-1}\mathrm{Tr}_i(\lambda) &= \sum_{\lambda \in F_i^*} \sum_{k=0}^{m_i - 1} \lambda^{q^k - 1} \\ &= \sum_{k=0}^{m_i - 1} \sum_{\lambda \in F_i^*} \lambda^{q^k - 1} \\ &= -1 \end{aligned}$$

since for any field F and for any non-negative integer s,

$$\sum_{\lambda \in F_i^*} \lambda^s = \begin{cases} -1, & \text{if } |F| - 1 \text{ divides } s; \\ 0, & \text{otherwise.} \end{cases}$$

This completes the proof of this lemma. ■

Lemma 3.5.13 *B_i is a non-singular bilinear form on $V_i \times V_{i'}$.*

Proof: Since B is non-singular and $V_i^{\perp} = \bigoplus_{j \neq i} V_j$ by Lemma 3.5.1, for any $u \in V_i$ there must be a $v \in V_{i'}$ such that $B(u, v) \neq 0$. Then by the previous lemma, $B_i(u, v) \neq 0$. Similarly, for any $v \in V_{i'}$ there is a $u \in V_i$ with $B_i(u, v) \neq 0$ and this shows that B_i is non-singular. The additivity of B_i in both variables is quite obvious. Finally, if $u \in V_i$, $v \in V_{i'}$ and $\mu \in F_i$ then

$$\begin{aligned} B_i(u\mu, v) &= \sum_{\lambda \in F_i^*} B(u\mu\lambda^{-1}, v)\lambda \\ &= \sum_{\lambda \in F_i^*} B(u(\mu\lambda^{-1}), v)(\lambda\mu^{-1})\mu \\ &= B_i(u, v)\mu \end{aligned}$$

with a change of variable from λ to $\lambda\mu^{-1}$. ∎

Lemma 3.5.14 *For any $1 \leq i \leq t$, $u \in V_i$, $v \in V_{i'}$, and for any $\varphi \in End_{\mathbf{F}\langle g \rangle}(V_i)$,*

$$B_i(u\varphi, v) = B_i(u, v\tau_i(\varphi)) .$$

Proof: Since φ is an $\mathbf{F}\langle g \rangle$-module endomorphism of V_i, φ commutes with any λ in F_i, and then

$$\begin{aligned} B_i(u, v\tau_i(\varphi)) &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}, v\tau_i(\varphi))\lambda \\ &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}, v\tau(\kappa_i(\varphi)))\lambda \\ &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}\kappa_i(\varphi), v)\lambda \\ &= \sum_{\lambda \in F_i^*} B(u\lambda^{-1}\varphi, v)\lambda \\ &= \sum_{\lambda \in F_i^*} B(u\varphi\lambda^{-1}, v)\lambda \\ &= B_i(u\varphi, v) \end{aligned}$$

as we wanted. ∎

Lemma 3.5.15 *Suppose $i \in I$ and $\varphi \in End_{\mathbf{F}\langle g\rangle}(V_i)$. Then*

$$\varphi \in I(V_i, B_i) \Longleftrightarrow \tau_i(\varphi) = \varphi^{-1}$$

Proof: This is an immediate corollary of the previous lemma. ■

Lemma 3.5.16 *For all $1 \leq i \leq t$ and $u \in V_i$, $v \in V_{i'}$*

$$B_{i'}(v,u) = \begin{cases} -\tau_i\big(B_i(u,v)\big), & \textit{if } B \textit{ is a symplectic form;} \\ \tau_i\big(B_i(u,v)\big), & \textit{if } B \textit{ is a unitary fom.} \end{cases}$$

Proof:

$$\begin{aligned} B_{i'}(v,u) &= \sum_{\gamma \in F_{i'}^*} B(v\gamma^{-1}, u)\gamma \\ &= \sum_{\gamma \in F_{i'}^*} B(v, u\tau_{i'}(\gamma)^{-1})\gamma \\ &= \sum_{\lambda \in F_i^*} B(v, u\lambda^{-1})\tau_i(\lambda) \\ &= \tau_i\Big(\sum_{\lambda \in F_i^*} B(v, u\lambda^{-1})^q \lambda\Big) \\ &= \begin{cases} -\tau_i\big(B_i(u,v)\big), & \text{if } B \text{ is a symplectic form;} \\ \tau_i\big(B_i(u,v)\big), & \text{if } B \text{ is a unitary fom.} \end{cases} \end{aligned}$$

Here we used the fact that $\tau_i(\alpha) = \alpha^q$ for any $\alpha \in \mathbf{F}$ (for details, see the proof of Lemma 3.5.10). ■

Theorem 3.5.17

$$|C_{I(V,B)}(g)| = \prod_{i \in I} |I(V_i, B_i)| \cdot \Big[\prod_{i \in J} |Aut_{\mathbf{F}\langle g\rangle}(V_i)|\Big]^{\frac{1}{2}} .$$

Proof: Suppose $\varphi \in C_{I(V,B)}(g)$. Then by Lemma 3.5.3

$$\varphi = \bigoplus_{i=1}^{t} \varphi_i$$

with some $\varphi_i \in \mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)$ and then by Lemma 3.5.7

$$\tau(\varphi) = \bigoplus_{i=1}^{t} \tau_i(\varphi_i) .$$

Now φ is in $I(V,B)$ if and only if $\tau(\varphi)=\varphi^{-1}$ which is the same as saying that for all $1\le i\le t$

$$\tau_i(\varphi_i)=\varphi_{i'}^{-1}\ .$$

If $i\in J$ then this condition means that $\varphi_i\in \mathrm{Aut}_{\mathbf{F}(g)}(V_i)$ can be chosen in any way and $\varphi_{i'}$ is then uniquely determined by φ_i. And if $i\in I$ then φ_i has to satisfy the property $\tau_i(\varphi_i)=\varphi_i^{-1}$, which is equivalent to saying that $\varphi_i\in I(V_i,B_i)$ (see Lemma 3.5.15). ■

Definition 3.5.18 *Define a positive real number* $\rho(V_i,B,g)$ *for each* $1\le i\le t$ *as follows. If* B *is a symplectic form and* $i\in I_1$ *then let*

$$\rho(V_i,B,g)=q^{\frac{n_i}{2}}\prod_{\substack{1\le k\le n_i\\ k\ \mathit{even}}}\left(1-\frac{1}{q^k}\right)\ .$$

If B *is a symplectic form and* $i\in I_2$ *then let*

$$\rho(V_i,B,g)=\prod_{k=1}^{n_i}\left(1-\frac{(-1)^k}{q^{\frac{m_i}{2}k}}\right)\ .$$

If B *is a symplectic form and* $i\in J$ *then let*

$$\rho(V_i,B,g)=\left[\prod_{k=1}^{n_i}\left(1-\frac{1}{q^{m_ik}}\right)\right]^{\frac{1}{2}}\ .$$

If B *is a unitary form and* $i\in I$ *then let*

$$\rho(V_i,B,g)=\prod_{k=1}^{n_i}\left(1-\frac{(-1)^k}{q^{m_ik}}\right)\ .$$

And finally, if B *is a unitary form and* $i\in J$ *then let*

$$\rho(V_i,B,g)=\left[\prod_{k=1}^{n_i}\left(1-\frac{1}{q^{2m_ik}}\right)\right]^{\frac{1}{2}}\ .$$

Theorem 3.5.19

$$|C_{I(V,B)}(g)|=\begin{cases} q^{\frac{1}{2}\sum_{i=1}^{t}m_in_i^2}\cdot\prod_{i=1}^{t}\rho(V_i,B,g), & \textit{if } B \textit{ is a symplectic form;}\\ q^{\sum_{i=1}^{t}m_in_i^2}\cdot\prod_{i=1}^{t}\rho(V_i,B,g), & \textit{if } B \textit{ is a unitary form.}\end{cases}$$

Proof: If B is a symplectic form and $i \in I_1$ then τ_i acts trivially on F_i and by Lemma 3.5.16 B_i is a symplectic form on V_i. Then it follows that

$$\begin{aligned}
|I(V_i, B_i)| &= |\mathrm{Sp}_{n_i}(q)| \\
&= q^{\frac{n_i^2+n_i}{2}} \prod_{\substack{1\le k\le n_i \\ k \text{ even}}} \left(1 - \frac{1}{q^k}\right) \\
&= q^{\frac{n_i^2}{2}} \rho(V_i, B, g) .
\end{aligned}$$

Notice that in the above case $m_i = 1$ so we could say

$$|I(V_i, B_i)| = q^{\frac{m_i n_i^2}{2}} \rho(V_i, B, g) .$$

If B is symplectic and $i \in I_2$ then τ_i acts as conjugation on F_i and if we fix an element $\delta \in F_i$ such that $\bar{\delta} = \delta^{-1}$ then by Lemma 3.5.16 δB_i is a unitary form on V_i, and therefore

$$\begin{aligned}
|I(V_i, B_i)| &= |I(V_i, \delta B_i)| \\
&= |\mathrm{GU}_{n_i}(q^{m_i})| \\
&= q^{\frac{m_i n_i^2}{2}} \prod_{k=1}^{n_i} \left(1 - \frac{(-1)^k}{q^{\frac{m_i}{2} k}}\right) \\
&= q^{\frac{m_i n_i^2}{2}} \rho(V_i, B, g) .
\end{aligned}$$

Also, if B symplectic and $i \in J$ then

$$\begin{aligned}
|\mathrm{Aut}_{\mathbf{F}\langle g\rangle}(V_i)|^{\frac{1}{2}} &= |\mathrm{GL}_{n_i}(q^{m_i})|^{\frac{1}{2}} \\
&= q^{\frac{m_i n_i^2}{2}} \left[\prod_{k=1}^{n_i} \left(1 - \frac{1}{q^{m_i k}}\right)\right]^{\frac{1}{2}} \\
&= q^{\frac{m_i n_i^2}{2}} \rho(V_i, B, g) .
\end{aligned}$$

Combining the above results with Theorem 3.5.17 we get that

$$|C_{I(V,B)}(g)| = q^{\frac{1}{2}\sum_{i=1}^{t} m_i n_i^2} \cdot \prod_{i=1}^{t} \rho(V_i, B, g) .$$

The other result for the case when B is a unitary form can be proven by the same way, first noticing that B_i is a non-singular unitary form on V_i by Lemma 3.5.16 for each $i \in I$ and then combining this fact with Theorem 3.5.17. ■

CHAPTER 4
FIXED POINT RATIOS ON THE COSETS OF EXTENSION FIELD TYPE SUBGROUPS

4.1 Notations and Some Technical Lemmas

Throughout the rest of this paper, we will use the following notations. Suppose G is a finite group, H is a subgroup of G and $g \in G$. By $N(G,H,g)$ we will denote the number of conjugates of H in G that contain g, $\mu(G,H,g)$ will denote the ratio of the fixed points of the action of g on the right cosets of H and $\mathcal{C}(G,H,g)$ will be the set of elements of H which are conjugate to g in G.

Lemma 4.1.1

$$\mu(G,H,g) = \frac{N(G,H,g)}{|G : N_G(H)|} \, .$$

Proof: The number of fixed points of the action of g on the cosets of H is

$$\frac{1}{|H|}|\{x \in G \,|\, Hxg = Hx\}| = \frac{1}{|H|}|\{x \in G \,|\, xgx^{-1} \in H\}| =$$

$$= \frac{1}{|H|}|\{x \in G \,|\, g \in x^{-1}Hx\}| = \frac{1}{|H|} \cdot N(G,H,g) \cdot |N_G(H)| \, .$$

To get the ratio of the fixed points, we have to divide this number by $|G : H|$, which gives us $\frac{|N_G(H)|}{|G|} \cdot N(G,H,g)$. ■

Lemma 4.1.2

$$N(G,H,g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G,H,g)|}{|N_G(H)|} \, ,$$

$$\mu(G,H,g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G,H,g)|}{|G|} \, .$$

Proof:

$$N(G,H,g) \cdot |N_G(H)| = |\{x \in G \,|\, g \in H^x\}| =$$

$$= |\{x \in G \mid g^x \in H\}| = |C_G(g)| \cdot |\mathcal{C}(G,H,g)| \,,$$

and the second statement follows from this and Lemma 4.1.1. ■

Lemma 4.1.3 *Let $g_1, g_2, \dots, g_k$ be representatives of the conjugacy classes of H which are conjugate to g in G. Then*

$$(a) \qquad N(G,H,g) = \frac{|H|}{|N_G(H)|} \cdot \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(g_i)|} \,,$$

$$(b) \qquad \mu(G,H,g) = \frac{|H|}{|G|} \cdot \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(g_i)|} \,.$$

Proof: Using the previous lemma,

$$N(G,H,g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G,H,g)|}{|N_G(H)|} =$$

$$= \frac{|C_G(g)|}{|N_G(H)|} \cdot \sum_{i=1}^{k} \frac{|H|}{|C_H(g_i)|} = \frac{|H|}{|N_G(H)|} \cdot \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H g_i|} \,,$$

and the statement for $\mu(G,H,g)$ now follows from Lemma 4.1.1. ■

Now we prove a few elementary facts about numbers that we will need later in this chapter.

Lemma 4.1.4 *For any prime power q and positive integer n,*

$$(a) \qquad \prod_{k=1}^{n} \left(1 - \frac{1}{q^k}\right) > \frac{q-2}{q-1} \,,$$

$$(b) \qquad \prod_{k=1}^{n} \left(1 - \frac{1}{q^k}\right) > \frac{1}{4} \,,$$

$$(c) \qquad 1 < \prod_{k=1}^{n} \left(1 - \frac{(-1)^k}{q^k}\right) \le \frac{q+1}{q} \,.$$

Proof: One can easily show by induction on n that $\prod_{k=1}^{n} \left(1 - \frac{1}{q^k}\right) \ge 1 - \sum_{k=1}^{n} \frac{1}{q^k}$, and therefore

$$\prod_{k=1}^{n} \left(1 - \frac{1}{q^k}\right) > 1 - \sum_{k=1}^{\infty} \frac{1}{q^k} = 1 - \frac{1}{q-1} = \frac{q-2}{q-1} \,.$$

This proves also (b), except when $q = 2$. For $q = 2$:

$$\prod_{k=1}^{n}\Big(1-\frac{1}{2^k}\Big) = \frac{1}{2}\prod_{k=2}^{n}\Big(1-\frac{1}{2^k}\Big) > \frac{1}{2}\Big(1-\sum_{k=2}^{\infty}\frac{1}{2^k}\Big) = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}\,.$$

Part (c) is trivial. ∎

Lemma 4.1.5 *For any prime power q and integer $r \geq 2$,*

$$\Big(\frac{q^r-2}{q^r-1}\Big)^{r-1} \geq \frac{1}{2}\,.$$

Proof: Since for any fixed r, $(\frac{q^r-2}{q^r-1})$ is an increasing function of q, it is sufficient to prove the statement for $q = 2$. In that case,

$$\Big(\frac{2^r-2}{2^r-1}\Big)^{r-1} = 2^{r-1}\Big(\frac{2^{r-1}-1}{2^r-1}\Big)^{r-1}\,,$$

so it is enough to show that

$$\Big(\frac{2^r-1}{2^{r-1}-1}\Big)^{r-1} = \Big(2+\frac{1}{2^{r-1}-1}\Big)^{r-1} \leq 2^r\,.$$

Rewrite the left hand side, by using the binomial coefficients, so

$$\begin{aligned}\Big(\frac{2^r-1}{2^{r-1}-1}\Big)^{r-1} &= 2^{r-1}+\sum_{i=1}^{r-1}\binom{r-1}{i}\frac{2^{r-1-i}}{(2^{r-1}-1)^i}\\ &< 2^{r-1}+\sum_{i=1}^{r-1}\binom{r-1}{i}\\ &= 2^{r-1}+(2^{r-1}-1) = 2^r-1 < 2^r\,,\end{aligned}$$

as wanted. ∎

4.2 Case I: p'-Elements Centralizing an Extension Field

Suppose V is a vector space of dimension d over $\mathbf{F}_q$, which is also a vector space of dimension $\frac{d}{r}$ over $\mathbf{F}_{q^r}$ with r being a prime divisor of d. To avoid confusion, we will denote V by $\hat{V}$ when we consider it as a vector space over $\mathbf{F}_{q^r}$. Let $G = \mathrm{GL}_{\mathbf{F}_q}(V)$, $H = \mathrm{GL}_{\mathbf{F}_{q^r}}(\hat{V})$ and $g \in H \setminus Z(G)$ an element of order o with $\gcd(o,p) = 1$.

Following the notations of Section 3.5, let

$$x^o - 1 = \prod_{i=1}^{t} f_i(x)$$

be the decomposition of the polynomial $x^o - 1$ into irreducible factors over $\mathbf{F}_{q^r}$ and for each $1 \le i \le t$, let

$$\hat{V}_i = \{v \in \hat{V} \mid v f_i(g) = 0\} \ .$$

Furthermore, let d_i be the dimension of $\hat{V}_i$ over $\mathbf{F}_{q^r}$, let m_i be the degree of $f_i(x)$ and let n_i be the number of direct summands in a decomposition of $\hat{V}_i$ into a direct sum of irreducible $\mathbf{F}_{q^r}\langle g\rangle$-modules. So $d_i = m_i n_i$ for all $1 \le i \le t$, $\sum_{i=1}^{t} m_i n_i = \frac{d}{r}$ and

$$\hat{V} = \hat{V}_1 \oplus \hat{V}_2 \oplus \ldots \oplus \hat{V}_t \ .$$

Define an equivalence relation on the set $\{1, 2, \ldots, t\}$ by saying that $i \sim j$ if $f_i(x)$ and $f_j(x)$ are conjugate polynomials over $\mathbf{F}_q$. Clearly, every equivalence class under this relation has cardinality 1 or r. Let $\{\mathcal{K}_j \mid 1 \le j \le s\}$ be set of equivalence classes with cardinality r, and $\mathcal{B} = \bigcup_{j=1}^{s} \mathcal{K}_j$, $\mathcal{A} = \{1, 2, \ldots, t\} \setminus \mathcal{B}$. So for any i, $i \in \mathcal{A}$ if $f_i(x) \in \mathbf{F}_q[x]$ and $i \in \mathcal{B}$ if $f_i(x) \notin \mathbf{F}_q[x]$. For $1 \le j \le s$, we will use the notations

$$n(j) = \sum_{i \in \mathcal{K}_j} n_i \ ,$$

$$m(j) = m_i \quad \text{for any } i \in \mathcal{K}_j \ ,$$

$$\text{and} \qquad V(j) = \bigoplus_{i \in \mathcal{K}_j} \hat{V}_i \ .$$

Notice that for any $i \in \mathcal{A}$, $V_i = \hat{V}_i$ is a direct sum of rn_i isomorphic irreducible $\mathbf{F}_q\langle g\rangle$-modules of dimension m_i over $\mathbf{F}_q$, and for any $1 \le j \le s$, $V(j)$ is a direct sum of $n(j)$ isomorphic irreducible $\mathbf{F}_q\langle g\rangle$-modules of dimension $rm(j)$ over $\mathbf{F}_q$. Furthermore, if W_1, W_2 are isomorphic irreducible direct summands of the $\mathbf{F}_q\langle g\rangle$-module V, then either $W_1, W_2 \le V_i$ for some $i \in \mathcal{A}$ or $W_1, W_2 \le V(j)$ for some $1 \le j \le s$.

If $\bar{g} \in H$ is an other element with order o, and we define the numbers $\bar{n}_i$ $(1 \le i \le t)$ and $\bar{n}(j)$ $(1 \le j \le s)$ as we defined n_i and $n(j)$ for g, then the necessary and sufficient condition for g and $\bar{g}$ to be conjugate to each other in H is that $n_i = \bar{n}_i$ for all $1 \leq i \leq t$. Furthermore, the necessary and sufficient condition for g and $\bar{g}$ to be conjugate in G is that $n_i = \bar{n}_i$ for all $i \in \mathcal{A}$ and $n(j) = \bar{n}(j)$ for all $1 \leq j \leq s$. This means that with the notation

$$\mathcal{S}_r(n) = \{(\bar{n}_1, \bar{n}_2, \dots, \bar{n}_r) \in \mathbf{Z}^r \mid 0 \leq \bar{n}_i \text{ for all } i \text{ and } \sum_{i=1}^{r} \bar{n}_i = n\}$$

there is a bijection between the elements of

$$\mathcal{S}_r(n(1)) \times \mathcal{S}_r(n(2)) \times \dots \times \mathcal{S}_r(n(s))$$

and the conjugacy classes of H which fall into the conjugacy class of g in G.

Then by Lemma 4.1.3 and using the fact that $|N_G(H) : H| = r$, we have that

$$N(G,H,g) = \frac{1}{r} \prod_{i \in \mathcal{A}} \frac{|\mathrm{GL}_{rn_i}(q^{m_i})|}{|\mathrm{GL}_{n_i}(q^{rm_i})|} \cdot \prod_{j=1}^{s} \Big[\sum_{(\bar{n}_1, \bar{n}_2, \dots, \bar{n}_r) \in \mathcal{S}_r(n(j))} \frac{|\mathrm{GL}_{n(j)}(q^{rm(j)})|}{\prod_{i=1}^{r} |\mathrm{GL}_{\bar{n}_i}(q^{rm(j)})|} \Big], \tag{4.1}$$

that is,

$$N(G,H,g) = \frac{1}{r} \prod_{i \in \mathcal{A}} \Big[q^{(r^2-r)m_i n_i^2} \prod_{\substack{1 \leq k \leq rn_i \\ r \nmid k}} \Big(1 - \frac{1}{q^{m_i k}}\Big) \Big] \cdot \prod_{j=1}^{s} \Big[\sum_{(\bar{n}_1, \bar{n}_2, \dots, \bar{n}_r) \in \mathcal{S}_r(n(j))} \frac{q^{rm(j)n(j)^2} \prod_{k=1}^{n(j)} \big(1 - \frac{1}{q^{rm(j)k}}\big)}{\prod_{i=1}^{r} q^{rm(j)\bar{n}_i^2} \big(\prod_{k=1}^{\bar{n}_i} \big(1 - \frac{1}{q^{rm(j)k}}\big) \big)} \Big]. \tag{4.2}$$

Our goal is now to give an upper bound to the right hand side of (4.2) with using only the variables d, r and q.

Lemma 4.2.1 *If m, n are integers with $n \geq 0$ and $m \geq 1$ then*

$$q^{(r^2-r)mn^2} \prod_{\substack{1 \leq k \leq rn \\ r \nmid k}} \Big(1 - \frac{1}{q^{mk}}\Big) \leq q^{(r^2-r)m^2n^2} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \Big(1 - \frac{1}{q^{k}}\Big).$$

Proof: If $n = 0$ or if $m = 1$ then equality holds. If $n > 0$ and $m \geq 2$ then $(r^2 - r)(m^2 - m)n^2 \geq 4$, so

$$q^{(r^2-r)mn^2} \leq q^4 \cdot q^{(r^2-r)m^2n^2}$$

while

$$\prod_{\substack{1 \leq k \leq rn \\ r \nmid k}} \left(1 - \frac{1}{q^{mk}}\right) \leq 1 \quad \text{and} \quad \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) \geq \frac{1}{4} \geq \frac{1}{q^2}$$

by Lemma 4.1.4. ■

Lemma 4.2.2 *If m, n are integers with $n \geq 0$ and $m \geq 2$ then*

$$q^{(r^2-r)mn^2} \prod_{\substack{1 \leq k \leq rn \\ r \nmid k}} \left(1 - \frac{1}{q^{mk}}\right) \leq q^{(r^2-r)(m^2n^2-mn)} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right),$$

except when $m = 2$ and $n = 1$.

Proof: If $n = 0$ then equality holds, so from now we will assume that n is positive. As in the proof of the previous lemma,

$$\prod_{\substack{1 \leq k \leq rn \\ r \nmid k}} \left(1 - \frac{1}{q^{mk}}\right) \leq 1 \quad \text{and} \quad \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) \geq \frac{1}{4} \geq \frac{1}{q^2},$$

so it is sufficient to show that

$$(r^2 - r)mn^2 \leq (r^2 - r)(m^2n^2 - mn) - 2 .$$

This inequality is equivalent to

$$2 \leq (r^2 - r)mn(mn - n - 1)$$

and this is clearly true whenever $m \geq 3$ or $m = 2$ and $n \geq 2$. ■

Lemma 4.2.3 *If $n = 1$ and m is any positive integer then*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} \left(\prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)\right)} = r .$$

Proof: For any $(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)$, $\bar{n}_i = 1$ for some $1 \leq i \leq r$ and $\bar{n}_j = 0$ for all $j \neq i$, and therefore

$$\frac{q^{rmn^2} \prod_{k=1}^{n} (1 - \frac{1}{q^{rmk}})}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} (\prod_{k=1}^{\bar{n}_i} (1 - \frac{1}{q^{rmk}}))} = 1 \ .$$

And of course, $|\mathcal{S}_r(n)| = |\mathcal{S}_r(1)| = r$. ■

Lemma 4.2.4 *If $n = 2$ and m is any positive integer then*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} (1 - \frac{1}{q^{rmk}})}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} (\prod_{k=1}^{\bar{n}_i} (1 - \frac{1}{q^{rmk}}))} = r + \binom{r}{2} q^{2rm} (1 + \frac{1}{q^{rm}}) \ .$$

Proof: For any $(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))$, either $\bar{n}_i = 2$ for some $1 \leq i \leq r$ and $\bar{n}_j = 0$ for all $j \neq i$, or $\bar{n}_i = \bar{n}_j = 1$ for some $1 \leq i < j \leq r$ and $\bar{n}_l = 0$ for all $l \notin \{i, j\}$. In the first case,

$$\frac{q^{rmn^2} \prod_{k=1}^{n} (1 - \frac{1}{q^{rmk}})}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} (\prod_{k=1}^{\bar{n}_i} (1 - \frac{1}{q^{rmk}}))} = 1 \ ,$$

and in the second case

$$\frac{q^{rmn^2} \prod_{k=1}^{n} (1 - \frac{1}{q^{rmk}})}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} (\prod_{k=1}^{\bar{n}_i} (1 - \frac{1}{q^{rmk}}))} = q^{2rm} \frac{(1 - \frac{1}{q^{rm}})(1 - \frac{1}{q^{2rm}})}{(1 - \frac{1}{q^{rm}})(1 - \frac{1}{q^{rm}})} = q^{2rm} (1 + \frac{1}{q^{rm}}) \ .$$

This completes the proof of this lemma. ■

Lemma 4.2.5 *If m, n are integers with $m \geq 1$, $n \geq 0$, and $r = 2$, then*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} (1 - \frac{1}{q^{rmk}})}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} (\prod_{k=1}^{\bar{n}_i} (1 - \frac{1}{q^{rmk}}))} < q^{mn^2+3} \ .$$

Proof: In this case, $\mathcal{S}_r(n) = \mathcal{S}_2(n) = \{(i, n-i) \in \mathbf{Z}^2 \,|\, 0 \leq i \leq n\}$, so

$$\begin{aligned}
\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2} \prod\limits_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod\limits_{i=1}^{r} q^{rm\bar{n}_i^2} \left(\prod\limits_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)\right)} &= \sum_{i=0}^{n} q^{2m(n^2-i^2-(n-i)^2)} \frac{\prod\limits_{k=i+1}^{n} \left(1 - \frac{1}{q^{2mk}}\right)}{\prod\limits_{k=1}^{n-i} \left(1 - \frac{1}{q^{2mk}}\right)} \\
&= \sum_{i=0}^{n} q^{4mi(n-i)} \frac{\prod_{k=i+1}^{n} \left(1 - \frac{1}{q^{2mk}}\right)}{\prod_{k=1}^{n-i} \left(1 - \frac{1}{q^{2mk}}\right)} \\
&\leq 2 \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} q^{4mi(n-i)+1} \\
&\leq 2 \sum_{k=0}^{mn^2} q^{k+1} < 2q^{mn^2+2} \\
&\leq q^{mn^2+3} \,,
\end{aligned}$$

as we wanted. ■

Lemma 4.2.6 *For any integers m, n with $m \geq 1$ and $n \geq 0$,*

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} \left(\prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)\right)} \leq q^{(r^2-r)m^2n^2} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) .$$

Proof: Since on the left hand side,

$$\frac{\prod_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} \prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)} = \frac{\prod_{k=\bar{n}_1+1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=2}^{r} \prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)} \leq \frac{1}{\left(\frac{q^r-2}{q^r-1}\right)^{r-1}} \leq q$$

for any $(\bar{n}_1, \bar{n}_2, \dots, \bar{n}_r) \in \mathcal{S}_r(n)$ (by using Lemmas 4.1.4 and 4.1.5), and on the right hand side,

$$\prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) \geq \frac{1}{q^2}$$

the inequality in the statement of this lemma certainly holds whenever

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2}}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2}} \cdot q \leq q^{(r^2-r)m^2n^2-2} . \tag{4.3}$$

And since $\sum_{i=1}^{r} \bar{n}_i^2 \geq \frac{n^2}{r}$ for any $(\bar{n}_1, \bar{n}_2, \dots, \bar{n}_r) \in \mathcal{S}_r(n)$ and $|\mathcal{S}_r(n)| = \binom{n+r-1}{r-1} \leq 2^{n+r-2} \leq q^{n+r-2}$, equation (4.3) is true if

$$q^{n+r-2} \cdot q^{rm(n^2-\frac{n^2}{r})} \cdot q \leq q^{(r^2-r)m^2n^2-2}$$

that is,

$$n + r + (r-1)mn^2 < (r^2 - r)m^2n^2 \; .$$

Dividing through by $(r^2 - r)m^2n^2$, this inequality is equivalent to

$$\frac{1}{(r^2 - r)m^2 n} + \frac{1}{(r-1)m^2n^2} + \frac{1}{rm} < 1 \; .$$

By simple calculations, it is easy to check that this inequality holds if $m \geq 2$ or if $m = 1$ and $r + n \geq 5$. This proves the lemma, except for the cases when $(m, n, r) = (1, 1, 2)$, $(1, 1, 3)$, or $(1, 2, 2)$.

If $m = n = 1$, then we refer to Lemma 4.2.3, according to which it is enough to show that

$$r \leq q^{(r^2-r)m^2n^2} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) = q^{(r^2-r)} \prod_{k=1}^{r-1} \left(1 - \frac{1}{q^k}\right) .$$

For $r = 2$, the right hand side is equal to $q^2(1 - \frac{1}{q})$, which is always at least 2, and if $r = 3$, then the right hand side is $q^6(1 - \frac{1}{q})(1 - \frac{1}{q^2})$, which is bigger than q^4, so also bigger than 3.

Finally, if $(m, n, r) = (1, 2, 2)$ then because of Lemma 4.2.4, it is sufficient to show that

$$2 + q^4\left(1 + \frac{1}{q^2}\right) \leq q^{(r^2-r)m^2n^2} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) = q^8 \prod_{\substack{1 \leq k \leq 4 \\ 2 \nmid k}} \left(1 - \frac{1}{q^k}\right) .$$

This is another obvious inequality for any q. ∎

Lemma 4.2.7 *For any positive integers m, n with $mn \geq 2$,*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} \left(\prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)\right)} \leq q^{(r^2-r)(m^2n^2-mn)} \prod_{\substack{1 \leq k \leq rmn \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) .$$

except when $(m, n, r) = (1, 2, 2)$, in which case

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n)} \frac{q^{rmn^2} \prod_{k=1}^{n} \left(1 - \frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2} \left(\prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{rmk}}\right)\right)} = 2 + q^2 + q^4 \; .$$

Proof: By using the same line of reasoning we started the previous lemma with, the inequality in the statement of this lemma holds whenever

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2}}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2}} \cdot q \leq q^{(r^2-r)(m^2n^2-mn)-2} \,. \tag{4.4}$$

Using the upper bounds $n^2 - \frac{n^2}{r}$ for $n^2 - \sum_{i=1}^{r} \bar{n}_i^2$ and q^{n+r-2} for $|\mathcal{S}_r(n)| = \binom{n+r-1}{r-1}$, the inequality (4.4) is true if

$$n + r + (r-1)mn^2 < (r^2-r)m^2n^2 - (r^2-r)mn \,.$$

By rearranging this, we get

$$\frac{1}{(r^2-r)m^2n} + \frac{1}{(r-1)m^2n^2} + \frac{1}{rm} + \frac{1}{mn} < 1 \,.$$

It is easy to check that this inequality holds whenever $m \geq 3$ or $m = 2$ and $n \geq 2$, or $m = 2$ and $r \geq 3$. It also holds if $r \geq 3$ and $n \geq 3$, or if at least one of them is greater than 3. Hence there are only a few cases left to check, namely those when $(m,n,r) = (1,2,2)$, $(1,2,3)$, $(1,3,2)$ or $(2,1,2)$.

If $(m,n,r) = (1,2,2)$ then by Lemma 4.2.4,

$$\begin{aligned}
\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2}\prod_{k=1}^{n}\left(1-\frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2}\left(\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{rmk}}\right)\right)} &= 2 + \binom{2}{2} q^4\left(1+\frac{1}{q^2}\right) \\
&= 2 + q^2 + q^4 \,.
\end{aligned}$$

If $(m,n,r) = (1,2,3)$ then by Lemma 4.2.4 it is enough to check that

$$3 + 3q^6\left(1+\frac{1}{q^3}\right) \leq q^{(r^2-r)(m^2n^2-mn)} \prod_{\substack{1\leq k\leq rmn \\ r\nmid k}} \left(1-\frac{1}{q^k}\right) = q^{12} \prod_{\substack{1\leq k\leq 6 \\ 3\nmid k}} \left(1-\frac{1}{q^k}\right) ,$$

which is clearly true.

If $(m,n,r) = (1,3,2)$ then $\mathcal{S}_r(n) = \mathcal{S}_2(3) = \{(0,3),(1,2),(2,1),(3,0)\}$ and

$$\begin{aligned}
\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n)} \frac{q^{rmn^2}\prod_{k=1}^{n}\left(1-\frac{1}{q^{rmk}}\right)}{\prod_{i=1}^{r} q^{rm\bar{n}_i^2}\left(\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{rmk}}\right)\right)} &= 2+2\cdot\frac{q^{18}\prod_{k=1}^{3}\left(1-\frac{1}{q^{2k}}\right)}{q^{10}\prod_{k=1}^{1}\left(1-\frac{1}{q^{2k}}\right)\prod_{k=1}^{2}\left(1-\frac{1}{q^{2k}}\right)} \\
&= 2+2q^8\cdot\frac{\left(1-\frac{1}{q^6}\right)}{\left(1-\frac{1}{q^2}\right)} \\
&= 2+2q^8\left(1+\frac{1}{q^2}+\frac{1}{q^4}\right).
\end{aligned}$$

On the other hand,

$$q^{(r^2-r)(m^2n^2-mn)}\prod_{\substack{1\le k\le rmn\\ r\nmid k}}\left(1-\frac{1}{q^k}\right) = q^{12}\prod_{\substack{1\le k\le 6\\ 2\nmid k}}\left(1-\frac{1}{q^k}\right),$$

so the statement of this lemma holds.

Finally, if $n=1$ then by Lemma 4.2.3, this lemma is true if

$$r \le q^{(r^2-r)(m^2n^2-mn)}\prod_{\substack{1\le k\le rmn\\ r\nmid k}}\left(1-\frac{1}{q^k}\right) = q^{(r^2-r)(m^2-m)}\prod_{\substack{1\le k\le rm\\ r\nmid k}}\left(1-\frac{1}{q^k}\right),$$

which holds whenever $m \ge 2$. ∎

Theorem 4.2.8 *Suppose $G \simeq GL_d(q)$ and $GL_{\frac{d}{r}}(q^r) \simeq H < G$ for some prime divisor r of d, and $g \in H$ is a p'-element, which is not in the center of G. Furthermore, assume that $r \ne d$. Then*

$$N(G,H,g) \le \frac{1}{r}q^{d^2-\frac{d^2}{r}-d(r-1)}\prod_{\substack{1\le k\le d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right),$$

except when

(a) $\quad 2 \ne r = \frac{d}{2}$, *in which case* $N(G,H,g) \le \frac{1}{r}q^{2r(r-1)}\prod_{k=1}^{r-1}\left(1-\frac{1}{q^{2k}}\right)$;

(b) $\quad 2 = r = \frac{d}{2}$, *in which case* $N(G,H,g) \le 1+\frac{q^2+q^4}{2}$.

Proof: Using Lemmas 4.2.1 and 4.2.6 for equation (4.2), we have

$$
\begin{aligned}
N(G,H,g) \leq \frac{1}{r}\prod_{i\in\mathcal{A}}\left[q^{(r^2-r)m_i^2n_i^2}\prod_{\substack{1\leq k\leq rm_in_i\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)\right]\cdot \\
\prod_{j=1}^{s}\left[q^{(r^2-r)m(j)^2n(j)^2}\prod_{\substack{1\leq k\leq rm(j)n(j)\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)\right] \\
\leq \frac{1}{r}q^{\sum_{i\in\mathcal{A}}(r^2-r)m_i^2n_i^2+\sum_{j=1}^{s}(r^2-r)m(j)^2n(j)^2}\prod_{\substack{1\leq k\leq\sum_{i\in\mathcal{A}}rm_in_i+\sum_{j=1}^{s}rm(j)n(j)\\ r\nmid k}}\left(1-\frac{1}{q^k}\right).
\end{aligned}
$$

Now, $\sum_{i\in\mathcal{A}} m_in_i+\sum_{j=1}^{s} m(j)n(j)=\frac{d}{r}$, and if at least two summands in this sum are non-zero, then

$$
\sum_{i\in\mathcal{A}} m_i^2n_i^2+\sum_{j=1}^{s} m(j)^2n(j)^2\leq(\frac{d}{r}-1)^2+1=\frac{d^2}{r^2}-\frac{2d}{r}+2
$$

and

$$
\begin{aligned}
N(G,H,g) &\leq \frac{1}{r}q^{(r^2-r)(\frac{d^2}{r^2}-\frac{2d}{r}+2)}\prod_{\substack{1\leq k\leq d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right) \\
&= \frac{1}{r}q^{d^2-\frac{d^2}{r}-2(d-r)(r-1)}\prod_{\substack{1\leq k\leq d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right) \\
&\leq \frac{1}{r}q^{d^2-\frac{d^2}{2}-d(r-1)}\prod_{\substack{1\leq k\leq d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right).
\end{aligned}
$$

We still have to consider the two cases: when $d=rm_in_i$ for some $i\in\mathcal{A}$ or $d=rm(j)n(j)$ for some $1\leq j\leq s$.

Suppose $d=rm_in_i$ for $i\in\mathcal{A}$. Then $m_i\geq 2$ because g is not a central element in G, and by Lemma 4.2.2, the statement of this lemma is true except when $n_i=1$ and $m_i=2$. In that case, by equation (4.2),

$$
N(G,H,g)=\frac{1}{r}q^{2(r^2-r)}\prod_{1\leq k\leq r-1}\left(1-\frac{1}{q^{2k}}\right).
$$

Finally, suppose that $d=rm(j)n(j)$ for some j. Then by Lemma 4.2.7,

$$
N(G,H,g)\leq\frac{1}{r}q^{(r^2-r)(\frac{d^2}{r^2}-\frac{d}{r})}\prod_{\substack{1\leq k\leq d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)=q^{d^2-\frac{d^2}{r}-d(r-1)}\prod_{\substack{1\leq k\leq d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right),
$$

except when $(m(j), n(j), r) = (1, 2, 2)$, in which case

$$N(G, H, g) = \frac{1}{2}(2 + q^2 + q^4) .$$

This completes the proof. ■

Theorem 4.2.9 *Suppose* $G \simeq GL_d(q)$ *and* $GL_{\frac{d}{r}}(q^r) \simeq H < G$ *for some prime divisor* r *of* d*, and* $g \in H$ *is a* p'*-element, which is not in the center of* G*. Furthermore, suppose that* $r \neq d$ *and* g *is not conjugate to any element in* $N_G(H) \setminus H$*. Then*

$$\mu(G, N_G(H), g) \leq \frac{1}{q^{d(r-1)}} ,$$

except when

(*a*) $2 \neq r = \dfrac{d}{2}$, *in which case* $\mu(G, N_G(H), g) \leq \dfrac{1}{q^{d(r-1)}} \displaystyle\prod_{\substack{1 \leq k \leq 2r \\ \gcd(k, 2r) = 1}} \frac{1}{\left(1 - \frac{1}{q^k}\right)}$;

(*b*) $2 = r = \dfrac{d}{2}$, *in which case* $\mu(G, N_G(H), g) \leq \dfrac{2 + q^2 + q^4}{q^4(q^3 - 1)(q - 1)}$.

Proof: Since by our assumption, g is not conjugate to any element in $N_G(H) \setminus H$, $N(G, H, g) = N(G, N_G(H), g)$. By Lemma 4.1.1,

$$\mu(G, N_G(H), g) = \frac{1}{|G : N_G(H)|} N(G, N_G(H), g)$$

and by an easy calculation,

$$|G : N_G(H)| = \frac{1}{r} \cdot q^{d^2 - \frac{d^2}{r}} \prod_{\substack{1 \leq k \leq d \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) .$$

Now everything follows from the previous theorem. ■

Lemma 4.2.10 *Suppose* $G \simeq GL_d(q)$*,* d *is a prime number,* $GL_1(q^d) \simeq H < G$*, and* $g \in H$ *is a* p'*-element, which is not in the center of* G*. Furthermore, suppose that* g *is not conjugate to any element in* $N_G(H) \setminus H$*. Then* $N(G, N_G(H), g) = 1$*.*

Proof: In equation (4.2), $1 = \frac{d}{r} = \sum_{i \in \mathcal{A}} m_i n_i + \sum_{j=1}^{s} m(j)n(j)$. Since $g \notin Z(G)$, this can only happen if $1 = m(j)n(j)$ for some $1 \leq j \leq s$ and $n(l) = 0$ for all $l \neq j$ and $n_i = 0$ for all $i \in \mathcal{A}$. Then by equation (4.2) and Lemma 4.2.3, $N(G, N_G(H), g) = N(G, H, g) = 1$. ∎

- - - - - - - - - - - - - - - - - - - -

Next, let $B : V \times V \to \mathbf{F}_q$ be a non-singular symplectic form on V, $G_1 \simeq \mathrm{Sp}_d(q)$ be the isometry group of (V, B) and $H_1 = H \cap G_1$. Assume that H_1 contains a Singer cycle of G_1 and $g \in H_1$. From Chapter 2, we know that H_1 is the isometry group of some non-singular form $\hat{B}$ on $\hat{V}$, that is either symplectic or unitary, according to whether $\frac{d}{r}$ is even or odd. Notice, that if $\hat{B}$ is unitary then $r = 2$. Furthermore, for the rest of this section we will assume that q is an odd prime power.

As we proved in Theorem 3.5.19,

$$|C_{H_1}(g)| = \prod_{i=1}^{t} q^{\frac{1}{2} r m_i n_i^2} \rho(\hat{V}_i, \hat{B}, g) ,$$

and

$$|C_{G_1}(g)| = \prod_{i \in \mathcal{A}} \left[q^{\frac{1}{2} m_i (r n_i)^2} \rho(V_i, B_i, g) \right] \cdot \prod_{j=1}^{s} \left[q^{\frac{1}{2} r m(j) n(j)^2} \rho(V(j), B, g) \right] ,$$

where

$$\rho(\hat{V}_i, \hat{B}, g) = \begin{cases} q^{\frac{1}{2} r n_i} \prod_{k=1}^{\frac{n_i}{2}} \left(1 - \frac{1}{q^{2rk}}\right) & \text{if } i \in I_1 \text{ and } \hat{B} \text{ is symplectic ;} \\ \prod_{k=1}^{n_i} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m_i k}}\right) & \text{if } i \in I_2 \text{ and } \hat{B} \text{ is symplectic ;} \\ \prod_{k=1}^{n_i} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m_i k}}\right) & \text{if } i \in I \text{ and } \hat{B} \text{ is unitary ;} \\ \left[\prod_{k=1}^{n_i} \left(1 - \frac{1}{q^{r m_i k}}\right)\right]^{\frac{1}{2}} & \text{if } i \in J \text{ ;} \end{cases} \tag{4.5}$$

$$\rho(V_i, B, g) = \begin{cases} q^{\frac{1}{2} r n_i} \prod_{k=1}^{\frac{1}{2} r n_i} \left(1 - \frac{1}{q^{2k}}\right) & \text{if } i \in I_1 \text{ ;} \\ \prod_{k=1}^{r n_i} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2} m_i k}}\right) & \text{if } i \in \mathcal{A} \cap I_2 \text{ ;} \\ \left[\prod_{k=1}^{r n_i} \left(1 - \frac{1}{q^{m_i k}}\right)\right]^{\frac{1}{2}} & \text{if } i \in \mathcal{A} \cap J \text{ ;} \end{cases} \tag{4.6}$$

$$\rho(V(j), B, g) = \begin{cases} \prod_{k=1}^{n(j)} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m(j) k}}\right) & \text{if for any } i \in \mathcal{K}_j,\ i' \in \mathcal{K}_j \text{ also ;} \\ \left[\prod_{k=1}^{n(j)} \left(1 - \frac{1}{q^{r m(j) k}}\right)\right]^{\frac{1}{2}} & \text{otherwise.} \end{cases} \tag{4.7}$$

Recall that for any $1 \leq i \leq t$, i' is the unique number between 1 and t such that the polynomial $x^{m_i} f_i(x^{-1})$ (or the polynomial $x^{m_i} \bar{f}_i(x^{-1})$, in the case when $\hat{B}$ is unitary) is a constant multiple of $f_{i'}(x)$; $I = \{i \mid i = i'\}$, $J = \{i \mid i \neq i'\}$, $I_1 = \{i \mid f_i(x) = x \pm 1\}$ and $I_2 = I \setminus I_1$.

As in the GL case, the conjugacy class of g in H_1 is characterized by the numbers n_i for $1 \leq i \leq t$ and the conjugacy class of g in G_1 is characterized by the numbers n_i for $i \in \mathcal{A}$ and $n(j)$ for $1 \leq j \leq s$. Therefore, by Lemma 4.1.3/(a),

$$N(G_1, H_1, g) \leq \frac{1}{r} \prod_{i \in \mathcal{A}} \left[q^{\frac{1}{2}(r^2 - r) m_i n_i^2} \frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} \right] \cdot$$

$$\prod_{j=1}^{s} \Big[\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2} r m(j) n(j)^2} \rho(V(j), B, g)}{\prod_{i=1}^{r} q^{\frac{1}{2} r m(j) \bar{n}_i^2} \bar{\rho}(j, \bar{n}_i)} \Big] \tag{4.8}$$

where

$$\bar{\rho}(j, \bar{n}_i) = \begin{cases} \prod_{k=1}^{\bar{n}_i} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m(j) k}}\right) & \text{if } \mathcal{K}_j \subseteq I_2 \text{ ;} \\ \left[\prod_{k=1}^{\bar{n}_i} \left(1 - \frac{1}{q^{r m(j) k}}\right)\right]^{\frac{1}{2}} & \text{if } \mathcal{K}_j \subseteq J. \end{cases} \tag{4.9}$$

Unlike in (4.2), in (4.8) we have only an inequality, because we may not need to use all the elements of the sets $\mathcal{S}_r(n(j))$ $(1 \leq j \leq s)$ to cover all the conjugacy classes of H_1 that fall into the conjugacy class of g in G_1.

In the following Lemmas we will obtain an upper bound for $N(G_1, H_1, g)$ using (4.8), that depends only on d, r and q.

Lemma 4.2.11 *(a) If $\hat{B}$ is symplectic and $i \in I_1$ then*

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} = \prod_{\substack{1 \leq k \leq \frac{1}{2} r n_i \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) .$$

(b) If $\hat{B}$ is unitary and $i \in I_1$ then

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} = q^{n_i} \prod_{k=1}^{n_i} \left(1 + \frac{(-1)^k}{q^k}\right) \leq q^{n_i} .$$

(c) If $i \in \mathcal{A} \cap I_2$ *then*

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} \leq 1 + \frac{1}{q} .$$

(d) If $i \in \mathcal{A} \cap J$ *then*

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} = \Big[\prod_{\substack{1 \leq k \leq rn_i \\ r \nmid k}} \Big(1 - \frac{1}{q^{m_i k}}\Big)\Big]^{\frac{1}{2}} .$$

(e) If $\mathcal{K}_j \subseteq I_2$ *and* $(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))$ *then*

$$\frac{\rho(V(j), B, g)}{\prod_{i=1}^{r} \bar{\rho}(j, \bar{n}_i)} \leq 1 .$$

(f) If $\mathcal{K}_j \subseteq J$ *and* $(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))$ *then*

$$\frac{\rho(V(j), B, g)}{\prod_{i=1}^{r} \bar{\rho}(j, \bar{n}_i)} \leq \sqrt{2} < \sqrt{q} .$$

Proof: Parts (a) and (d) are quite straightforward from equations (4.6) and (4.5).

(b) In this case $m_i = 1$ and $r = 2$, so from (4.6) and (4.5),

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)} = \frac{q^{n_i} \prod_{k=1}^{n_i} \big(1 - \frac{1}{q^{2k}}\big)}{\prod_{k=1}^{n_i} \big(1 - \frac{(-1)^k}{q^k}\big)} = q^{n_i} \prod_{k=1}^{n_i} \Big(1 + \frac{(-1)^k}{q^k}\Big) .$$

(c) Notice that in this case m_i is even. By (4.6),

$$\rho(V_i, B, g) = \prod_{k=1}^{rn_i} \Big(1 - \frac{(-1)^k}{q^{\frac{1}{2} m_i k}}\Big) \leq 1 + \frac{1}{q}$$

and by (4.5),

$$\rho(\hat{V}_i, \hat{B}, g) = \prod_{k=1}^{n_i} \Big(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m_i k}}\Big) \geq 1 .$$

(e) By equations (4.7) and (4.9) what we need is that

$$\prod_{k=1}^{n(j)} \Big(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m(j) k}}\Big) \leq \prod_{i=1}^{r} \prod_{k=1}^{\bar{n}_i} \Big(1 - \frac{(-1)^k}{q^{\frac{1}{2} r m(j) k}}\Big)$$

and this is true simply because for all positive integers l, n and for any prime power q,

$$\prod_{k=l+1}^{l+n} \Big(1 - \frac{(-1)^k}{q^k}\Big) \leq \prod_{k=1}^{n} \Big(1 - \frac{(-1)^k}{q^k}\Big) .$$

(f) By equations (4.7) and (4.9), either

$$\begin{aligned}
\frac{\rho(V(j),B,g)}{\prod_{i=1}^{r}\bar{\rho}(j,\bar{n}_i)} &= \Big[\frac{\prod_{k=1}^{n(j)}\left(1-\frac{1}{q^{rm(j)k}}\right)}{\prod_{k=1}^{r}\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{rm(j)k}}\right)}\Big]^{\frac{1}{2}} \\
&\leq \Big[\frac{\prod_{k=\bar{n}_1+1}^{n(j)}\left(1-\frac{1}{q^{rm(j)k}}\right)}{\prod_{k=2}^{r}\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{rm(j)k}}\right)}\Big]^{\frac{1}{2}} \\
&\leq \left[\frac{1}{\left(\frac{q^r-2}{q^r-1}\right)^{r-1}}\right]^{\frac{1}{2}} \\
&\leq 2^{\frac{1}{2}}
\end{aligned}$$

(here in the last two lines we used Lemmas 4.1.4/(a) and 4.1.5), or for any i in $\mathcal{K}_j$, i' is also in $\mathcal{K}_j$, in which case $r=2$ (because $|\mathcal{K}_j| = r$ for any $\mathcal{K}_j \subseteq J$, and the above mentioned condition implies that $|\mathcal{K}_j|$ is even), and then

$$\frac{\rho(V(j),B,g)}{\prod_{i=1}^{r}\bar{\rho}(j,\bar{n}_i)} = \frac{\prod_{k=1}^{n(j)}\left(1-\frac{(-1)^k}{q^{m(j)k}}\right)}{\left[\prod_{i=1}^{2}\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{2m(j)k}}\right)\right]^{\frac{1}{2}}}\,.$$

If $n(j)=1$ then this is equal to

$$\frac{1+\frac{1}{q^{m(j)}}}{\left[1-\frac{1}{q^{2m(j)}}\right]^{\frac{1}{2}}} = \left[\frac{1+\frac{1}{q^{m(j)}}}{1-\frac{1}{q^{m(j)}}}\right]^{\frac{1}{2}} = \left[\frac{q^{m(j)}+1}{q^{m(j)}-1}\right]^{\frac{1}{2}},$$

and this is less than or equal to $\left[\frac{3+1}{3-1}\right]^{\frac{1}{2}} = \sqrt{2}$. If $n(j) \geq 2$ then

$$\prod_{k=1}^{n(j)}\left(1-\frac{(-1)^k}{q^{m(j)k}}\right) \leq \left(1+\frac{1}{q^{m(j)}}\right)\left(1-\frac{1}{q^{2m(j)}}\right)\left(1+\frac{1}{q^{3m(j)}}\right) \leq \frac{4}{3}\cdot\frac{8}{9}\cdot\frac{28}{27}\,,$$

while

$$\left[\prod_{i=1}^{2}\prod_{k=1}^{\bar{n}_i}\left(1-\frac{1}{q^{2m(j)k}}\right)\right]^{\frac{1}{2}} \geq \frac{q^{2m(j)}-2}{q^{2m(j)}-1} \geq \frac{3^2-2}{3^2-1} = \frac{7}{8}\,,$$

and this implies

$$\frac{\rho(V(j),B,g)}{\prod_{i=1}^{r}\bar{\rho}(j,\bar{n}_i)} \leq \frac{4}{3}\cdot\frac{8}{9}\cdot\frac{28}{27}\cdot\frac{8}{7} = \frac{1024}{729} < \sqrt{2}\,.$$

This completes the proof of this lemma. ■

Lemma 4.2.12 *(a) If $\hat{B}$ is symplectic and $i \in \mathcal{A} \cap I$, or if $\hat{B}$ is unitary and $i \in \mathcal{A} \cap I_2$ then*

$$q^{\frac{1}{2}(r^2-r)m_in_i^2}\frac{\rho(V_i,B,g)}{\rho(\hat{V}_i,\hat{B},g)} \leq q^{\frac{1}{2}(r^2-r)m_i^2n_i^2} \prod_{\substack{1\leq k\leq \frac{1}{2}rm_in_i \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right).$$

(b) If $i \in \mathcal{A} \cap I_2$ then

$$q^{\frac{1}{2}(r^2-r)m_in_i^2}\frac{\rho(V_i,B,g)}{\rho(\hat{V}_i,\hat{B},g)} \leq q^{\frac{1}{2}(r^2-r)(m_i^2n_i^2-m_in_i)} \prod_{\substack{1\leq k\leq \frac{1}{2}rm_in_i \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right),$$

except when $m_i = 2$ and $n_i = 1$.

Proof: If $n_i = 0$ then these statements are obvious, so from now we will assume that n_i is positive.

If $i \in I_1$ then $m_i = 1$ and because of Lemma 4.2.11/(a), equality holds in the statement.

If $i \in \mathcal{A} \cap I_2$ then $m_i \geq 2$ and by Lemma 4.2.11/(c)

$$\frac{\rho(V_i,B,g)}{\rho(\hat{V}_i,\hat{B},g)} \leq 1+\frac{1}{q} \leq \frac{4}{3}$$

and by Lemma 4.1.4/(a),

$$\prod_{\substack{1\leq k\leq \frac{1}{2}rm_in_i \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right) > \frac{q^2-2}{q^2-1} \geq \frac{7}{8}.$$

Since $\frac{4}{3}\cdot\frac{8}{7}=\frac{32}{21}\leq\sqrt{q}$, (a) holds whenever

$$\frac{1}{2}(r^2-r)m_in_i^2+\frac{1}{2} \leq \frac{1}{2}(r^2-r)m_i^2n_i^2,$$

and (b) holds whenever

$$\frac{1}{2}(r^2-r)m_in_i^2+\frac{1}{2} \leq \frac{1}{2}(r^2-r)(m_i^2n_i^2-m_in_i).$$

The first inequality is equivalent to $1 \leq r(r-1)m_in_i^2(m_i-1)$, and is always true since $m_i \geq 2$; the second inequality is equivalent to $1 \leq r(r-1)m_in_i(m_in_i-n_i-1)$, and this is true unless $m_i = 2$ and $n_i = 1$. If $m_i = 2$ and $n_i = 1$ then the left hand side of statement (b) is

$$q^{r^2-r} \frac{\prod_{k=1}^{r} \left(1 - \frac{(-1)^k}{q^k}\right)}{1 + \frac{1}{q^r}} ,$$

and the right hand side is

$$q^{r^2-r} \prod_{\substack{1 \leq k \leq 2r \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) ,$$

so the inequality does not hold. ■

Lemma 4.2.13 *If* $i \in \mathcal{A} \cap J$ *then*

$$\left[q^{\frac{1}{2}(r^2-r)m_i n_i^2} \frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)}\right] \cdot \left[q^{\frac{1}{2}(r^2-r)m_{i'} n_{i'}^2} \frac{\rho(V_{i'}, B, g)}{\rho(\hat{V}_{i'}, \hat{B}, g)}\right] \leq$$
$$q^{\frac{1}{2}(r^2-r)(m_i^2 n_i^2 + m_{i'}^2 n_{i'}^2)} \prod_{\substack{1 \leq k \leq \frac{1}{2}(r m_i n_i + r m_{i'} n_{i'}) \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) .$$

Proof: First, if $n_i = n_{i'} = 0$ then there is nothing to prove, so from now we assume that n_i is positive. We should notice that $m_i = m_{i'}$ and $n_i = n_{i'}$ for all i. Therefore, the left hand side of the statement is actually

$$q^{(r^2-r)m_i n_i^2} \left(\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, \hat{B}, g)}\right)^2 = q^{(r^2-r)m_i n_i^2} \prod_{\substack{1 \leq k \leq r n_i \\ r \nmid k}} \left(1 - \frac{1}{q^{m_i k}}\right) ,$$

while on the right hand side,

$$\frac{1}{2}(r^2 - r)(m_i^2 n_i^2 + m_{i'}^2 n_{i'}^2) = (r^2 - r) m_i^2 n_i^2$$

and

$$\frac{1}{2}(r m_i n_i + r m_{i'} n_{i'}) = r m_i n_i \ .$$

If $m_i = 1$ then the statement simply follows from the fact that

$$\prod_{\substack{1 \leq k \leq r n_i \\ r \nmid k}} \left(1 - \frac{1}{q^k}\right) < \prod_{\substack{1 \leq k \leq r n_i \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) ,$$

and if $m_i \geq 2$, then by using the bounds

$$\prod_{\substack{1 \leq k \leq rn_i \\ r \nmid k}} \left(1 - \frac{1}{q^{m_i k}}\right) \leq 1 \quad \text{and} \quad \prod_{\substack{1 \leq k \leq rm_i n_i \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) \geq \frac{q^2-2}{q^2-1} > q^{-1} ,$$

the inequality of this lemma is true whenever

$$q^{(r^2-r)m_i n_i^2} \leq q^{(r^2-r)m_i^2 n_i^2 - 1}$$

that is, $1 \leq (r^2-r)m_i(m_i-1)n_i^2$. This obviously holds for $m_i \geq 2$ and $n_i \geq 1$. ■

Lemma 4.2.14 *If* $n(j) = 1$ *then*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2} \rho(V(j), B, g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2} \bar{\rho}(j, \bar{n}_i)} = r .$$

Proof: The proof has exactly the same simple line of reasoning as the proof of Lemma 4.2.3. ■

Lemma 4.2.15 *If* $n(j) = 2$ *then*

$$\sum_{(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2} \rho(V(j), B, g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2} \bar{\rho}(j, \bar{n}_i)} < \left(r + \binom{r}{2} q^{rm(j)}\right) \cdot \sqrt{2} < q^{rm(j)+r-1} .$$

Proof: For any $(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_r) \in \mathcal{S}_r(n(j))$, either $\bar{n}_i = 2$ for some $1 \leq i \leq r$ and $\bar{n}_j = 0$ for all $j \neq i$, or $\bar{n}_i = \bar{n}_j = 1$ for some $1 \leq i < j \leq r$ and $\bar{n}_l = 0$ for all $l \notin \{i, j\}$. In the first case,

$$\frac{q^{\frac{1}{2}rm(j)n(j)^2}}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}} = 1 ,$$

and in the second case,

$$\frac{q^{\frac{1}{2}rm(j)n(j)^2}}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}} = q^{rm(j)} .$$

Furthermore, by Lemma 4.2.11/(e) and (f),

$$\frac{\rho(V(j), B, g)}{\prod_{i=1}^{r} \bar{\rho}(j, \bar{n}_i)} \leq \sqrt{2} .$$

This implies

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} \le \left(r+\binom{r}{2}q^{rm(j)}\right)\cdot\sqrt{2}\,,$$

and

$$\left(r+\binom{r}{2}q^{rm(j)}\right)\cdot\sqrt{2} = (2r+r(r-1)q^{rm(j)})\frac{1}{\sqrt{2}} < r^2q^{rm(j)}\frac{1}{\sqrt{2}} < q^{rm(j)+r-1}$$

since $\frac{r^2}{\sqrt{2}} < 3^{r-1} \le q^{r-1}$. ■

Lemma 4.2.16 *(a) If $r = 2$ then for any $1 \le j \le s$,*

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} < q^{\frac{1}{2}m(j)n(j)^2+\frac{3}{2}}\,.$$

(b) If $r = 2$ and $n(j) = 3$ then

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} < q^{4m(j)+1}+q\,.$$

Proof: In this case, $\mathcal{S}_r(n(j)) = \mathcal{S}_2(n(j)) = \{(i, n(j)-i) \,|\, 0 \le i \le n(j)\}$, and by Lemma 4.2.11,

$$\frac{\rho(V(j),B,g)}{\prod_{i=1}^{2}\bar{\rho}(j,\bar{n}_i)} \le 2^{\frac{1}{2}}\,.$$

Therefore,

$$\begin{aligned}
\sum_{(\bar{n}_1,\bar{n}_2)\in\mathcal{S}_2(n(j))} \frac{q^{m(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{2} q^{m(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} &\le \sum_{i=0}^{n(j)} q^{m(j)(n(j)^2-i^2-(n(j)-i)^2)}\cdot 2^{\frac{1}{2}} \\
&= \sum_{i=0}^{n(j)} q^{2m(j)i(n(j)-i)}\cdot 2^{\frac{1}{2}} \\
&\le 2\sum_{i=0}^{\lfloor\frac{n(j)}{2}\rfloor} q^{2m(j)i(n(j)-i)}\cdot 2^{\frac{1}{2}} \\
&\le 2\sum_{k=0}^{\lfloor\frac{1}{2}m(j)n(j)^2\rfloor} q^{k}\cdot 2^{\frac{1}{2}} \\
&= \frac{2}{q-1}\left(q^{\lfloor\frac{1}{2}m(j)n(j)^2\rfloor+1}-1\right)\cdot 2^{\frac{1}{2}} \\
&< q^{\frac{1}{2}m(j)n(j)^2+\frac{3}{2}}\,.
\end{aligned}$$

If $n(j) = 3$, then as above,

$$\begin{aligned}\sum_{(\bar{n}_1,\bar{n}_2)\in\mathcal{S}_2(n(j))} \frac{q^{m(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{2} q^{m(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} &\le \sum_{i=0}^{3} q^{2m(j)i(3-i)}\cdot 2^{\frac{1}{2}} \\ &= (1+q^{4m(j)})\cdot 2^{\frac{3}{2}} \\ &< q+q^{4m(j)+1} ,\end{aligned}$$

as stated. ■

Lemma 4.2.17 *(a) For any* $1 \le j \le s$,

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} \le q^{\frac{1}{2}(r^2-r)m(j)^2n(j)^2-\frac{1}{2}} ,$$

except when $(m(j),n(j),r,q) = (1,1,2,3)$.

(b) If $m(j)n(j) \ge 2$ *and* $(m(j),n(j),r) \ne (1,2,2)$ *then*

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} \le q^{\frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))-\frac{1}{2}} .$$

Proof: Like in the GL case, we can get a general upper bound for

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} .$$

For any $(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))$, $n(j)^2-\sum_{i=1}^{r}\bar{n}_i^2 \le \frac{r-1}{r}n(j)^2$ and the cardinality of $\mathcal{S}_r(n(j))$ is $\binom{n(j)+r-1}{r-1} \le 2^{n(j)+r-2} < q^{\frac{2}{3}(n(j)+r-2)} < q^{\frac{2}{3}n(j)+\frac{2}{3}r-1}$. Furthermore, by Lemma 4.2.11,

$$\frac{\rho(V(j),B,g)}{\prod_{i=1}^{r}\bar{\rho}(j,\bar{n}_i)} < q^{\frac{1}{2}}$$

for all $(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))$. Therefore,

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,n(j),\bar{n}_i)} < q^{\frac{2}{3}n(j)+\frac{2}{3}r-1}\cdot q^{\frac{1}{2}(r-1)m(j)n(j)^2}\cdot q^{\frac{1}{2}} .$$

This implies that (a) holds whenever

$$\frac{2}{3}n(j)+\frac{2}{3}r-1+\frac{1}{2}(r-1)m(j)n(j)^2+\frac{1}{2} \le \frac{1}{2}(r^2-r)m(j)^2n(j)^2-\frac{1}{2} ,$$

---

that is

$$\frac{4}{3}n(j)+\frac{4}{3}r+(r-1)m(j)n(j)^2 \le (r^2-r)m(j)^2n(j)^2 ,$$

and (b) holds whenever

$$\frac{2}{3}n(j)+\frac{2}{3}r-1+\frac{1}{2}(r-1)m(j)n(j)^2+\frac{1}{2} \le \frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))-\frac{1}{2} ,$$

that is

$$\frac{4}{3}n(j)+\frac{4}{3}r+(r-1)m(j)n(j)^2 \le (r^2-r)m(j)^2n(j)^2-(r^2-r)m(j)n(j) .$$

By dividing through with $(r^2-r)m(j)^2n(j)^2$, we get

$$\frac{4}{3r(r-1)m(j)^2n(j)}+\frac{4}{3(r-1)m(j)^2n(j)^2}+\frac{1}{rm(j)} \le 1 , \tag{4.10}$$

and

$$\frac{4}{3r(r-1)m(j)^2n(j)}+\frac{4}{3(r-1)m(j)^2n(j)^2}+\frac{1}{rm(j)}+\frac{1}{m(j)n(j)} \le 1 , \tag{4.11}$$

respectively. It is easy to check that (4.10) holds if $m(j) \ge 2$, or if $n(j) \ge 3$, or if $m(j)=1$, $n(j)=2$ and $r \ge 3$. Also, (4.11) is true whenever $n(j) \ge 3$ and $r \ge 3$.

Now assume that $r=2$. Then by Lemma 4.2.16,

$$\frac{1}{2}m(j)n(j)^2+\frac{3}{2} \le m(j)^2n(j)^2-m(j)n(j)-\frac{1}{2}$$

is a sufficient condition for (b). This inequality is equivalent to

$$\frac{1}{2}m(j)n(j)^2+m(j)n(j)+2 \le m(j)^2n(j)^2 ,$$

$$\frac{1}{2m(j)}+\frac{1}{m(j)n(j)}+\frac{2}{m(j)^2n(j)^2} \le 1 ,$$

which holds whenever $n(j) \ge 3$, except the case $(m(j),n(j))=(1,3)$. For the case $(m(j),n(j),r)=(1,3,2)$, by Lemma 4.2.16/(b),

$$\sum_{(\bar{n}_1,\bar{n}_2,\dots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} < q^5+q ,$$

while

$$q^{\frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))-\frac{1}{2}} = q^{5\frac{1}{2}} .$$

And it is true that $q^5 + q < q^{5\frac{1}{2}}$. This proves (b) for the $r = 2$, $n(j) \geq 3$ case. As for (a) when $r = 2$, from Lemma 4.2.16/(a),

$$\frac{1}{2}m(j)n(j)^2 + \frac{3}{2} \leq m(j)^2n(j)^2 - \frac{1}{2} ,$$

that is,

$$\frac{1}{2m(j)} + \frac{2}{m(j)^2n(j)^2} \leq 1$$

is a sufficient condition that is always true, except when $(m(j), n(j)) = (1, 1)$.

Now assume that $n(j) = 2$. Then by Lemma 4.2.15,

$$rm(j) + r - 1 \leq \frac{1}{2}(r^2 - r)(4m(j)^2 - 2m(j)) - \frac{1}{2} = r(r-1)(2m(j)^2 - m(j)) - \frac{1}{2}$$

is a sufficient condition for (b). This is equivalent to

$$r(m(j) + 1) \leq r(r-1)m(j)(2m(j) - 1) ,$$

that is,

$$m(j) + 1 \leq (r-1)m(j)(2m(j) - 1) .$$

Again, this is always true, except when $(m(j), r) = (1, 2)$.

Next, assume that $n(j) = 1$. Then by Lemma 4.2.14, (a) is equivalent to

$$r \leq q^{\frac{1}{2}(r^2-r)m(j)^2n(j)^2-\frac{1}{2}}$$

and (b) is equivalent to

$$r \leq q^{\frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))-\frac{1}{2}} .$$

These inequalities always hold if $m(j)n(j) \geq 2$, since in that case,

$$q^{\frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))-\frac{1}{2}} \geq q^{r^2-r-\frac{1}{2}} \geq 3^{r-\frac{1}{2}} > r .$$

The first inequality also holds for $(m(j), n(j)) = (1, 1)$, except when $r = 2$ and $q = 3$. The proof of this lemma is now complete. ■

Lemma 4.2.18 *(a) For any* $1 \leq j \leq s$*,*

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} \leq q^{\frac{1}{2}(r^2-r)m(j)^2n(j)^2}\prod_{k=1}^{\infty}\left(1-\frac{1}{q^{2k}}\right).$$

(b) If $m(j)n(j) \geq 2$ *and* $(m(j),n(j),r) \neq (1,2,2)$ *then*

$$\sum_{(\bar{n}_1,\bar{n}_2,\ldots,\bar{n}_r)\in\mathcal{S}_r(n(j))} \frac{q^{\frac{1}{2}rm(j)n(j)^2}\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)\bar{n}_i^2}\bar{\rho}(j,\bar{n}_i)} \leq$$

$$q^{\frac{1}{2}(r^2-r)(m(j)^2n(j)^2-m(j)n(j))}\prod_{k=1}^{\infty}\left(1-\frac{1}{q^{2k}}\right).$$

Proof: Except for (a), when $(m(j),n(j),r,q)=(1,1,2,3)$, it follows from the previous lemma, since

$$\prod_{k=1}^{\infty}\left(1-\frac{1}{q^{2k}}\right) \geq \frac{q^2-2}{q^2-1} \geq q^{-\frac{1}{2}}.$$

For the case $(m(j),n(j),r,q)=(1,1,2,3)$,

$$q^{\frac{1}{2}(r^2-r)m(j)^2n(j)^2}\prod_{k=1}^{\infty}\left(1-\frac{1}{q^{2k}}\right) \geq 3\cdot\frac{3^2-2}{3^2-1} = \frac{21}{8} > 2 = r,$$

and the left hand side of the inequality in (a) is equal to r, by Lemma 4.2.14. ∎

Theorem 4.2.19 *Suppose* $G \simeq Sp_d(q)$ *and* $Sp_{\frac{d}{r}}(q^r) \simeq H < G$ *for some prime divisor* r *of* d*, and* $g \in H$ *is a* p'*-element, which is not in the center of* G*. Furthermore, assume that* $r \neq d$*.*

$$(a) \qquad \text{If } r \neq \frac{d}{2} \text{ then } N(G,H,g) \leq \frac{1}{r}q^{\frac{d^2}{2}-\frac{d^2}{2r}-\frac{d}{2}(r-1)}\prod_{\substack{1\leq k\leq\frac{d}{2}\\ r\nmid k}}\left(1-\frac{1}{q^{2k}}\right).$$

$$(b) \qquad \text{If } r = \frac{d}{2} \text{ then } N(G,H,g) \leq \frac{1}{r}q^{r(r-1)}\prod_{k=1}^{r-1}\left(1-\frac{(-1)^k}{q^k}\right).$$

Proof: Using Lemmas 4.2.12, 4.2.13 and 4.2.18/(a) for equation (4.8), like in the proof of Theorem 4.2.8 we get that

$$N(G,H,g) \leq \frac{1}{r}q^{\frac{1}{2}(r^2-r)\left[\sum_{i\in A} m_i^2n_i^2\right]+\frac{1}{2}(r^2-r)\left[\sum_{j=1}^{s} m(j)^2n(j)^2\right]}\prod_{\substack{1\leq k\leq\frac{d}{2}\\ r\nmid k}}\left(1-\frac{1}{q^{2k}}\right).$$

Now, $\sum_{i\in\mathcal{A}} m_i n_i + \sum_{j=1}^{s} m(j)n(j) = \frac{d}{r}$, and if at least two summands in this sum are non-zero, then

$$\sum_{i\in\mathcal{A}} m_i^2 n_i^2 + \sum_{j=1}^{s} m(j)^2 n(j)^2 \leq (\frac{d}{r}-1)^2 + 1 = \frac{d^2}{r^2} - \frac{2d}{r} + 2$$

and

$$\begin{aligned} N(G,H,g) &\leq \frac{1}{r} q^{\frac{1}{2}(r^2-r)(\frac{d^2}{r^2}-\frac{2d}{r}+2)} \prod_{\substack{1\leq k\leq \frac{d}{2} \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right) \\ &= \frac{1}{r} q^{\frac{d^2}{2}-\frac{d^2}{2r}-(d-r)(r-1)} \prod_{\substack{1\leq k\leq \frac{d}{2} \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right) \\ &\leq \frac{1}{r} q^{\frac{d^2}{2}-\frac{d^2}{2r}-\frac{d}{2}(r-1)} \prod_{\substack{1\leq k\leq \frac{d}{2} \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right). \end{aligned}$$

We still have to consider the two cases, when $d = rm_i n_i$ for some $i \in \mathcal{A}$ or $d = rm(j)n(j)$ for some $1 \leq j \leq s$.

Suppose $d = rm_i n_i$ for $i \in \mathcal{A}$. Then $i = i'$ (since $n_i = n_{i'}$, in general), so $i \in I$ and $m_i \geq 2$ because g is not a central element in G. Now by Lemma 4.2.12/(b), the statement of this lemma is true except when $n_i = 1$ and $m_i = 2$. In that case, by equations (4.8), (4.6) and (4.5),

$$N(G,H,g) = \frac{1}{r} q^{r^2-r} \frac{\prod_{k=1}^{r}\left(1-\frac{(-1)^k}{q^k}\right)}{1+\frac{1}{q^r}} \leq \frac{1}{r} q^{r^2-r} \prod_{k=1}^{r-1}\left(1-\frac{(-1)^k}{q^k}\right).$$

Finally, suppose that $d = rm(j)n(j)$ for some j. (In other words, this means $V = V(j)$.) Then by Lemma 4.2.18/(b),

$$N(G,H,g) \leq \frac{1}{r} q^{\frac{1}{2}(r^2-r)(\frac{d^2}{r^2}-\frac{d}{r})} \prod_{k=1}^{\infty}\left(1-\frac{1}{q^{2k}}\right) = q^{\frac{d^2}{2}-\frac{d^2}{2r}-\frac{d}{2}(r-1)} \prod_{\substack{1\leq k\leq \frac{d}{2} \\ r\nmid k}} \left(1-\frac{1}{q^{2k}}\right),$$

except when $(m(j), n(j), r) = (1,2,2)$. In that case, $|\mathcal{K}_j| = 2$, so either $\mathcal{K}_j = \{i, i'\}$ for some $i \in J$, or $\mathcal{K}_j = \{i, l\}$ with $i, l \in I$. (Recall, that $n_i = n_{i'}$ for all $1 \leq i \leq t$, so $V = V(j)$ implies that $i' \in \mathcal{K}_j$ for any $i \in \mathcal{K}_j$.)

If $\mathcal{K}_j = \{i, i'\}$ for some $i \in J$, then $n_i = n_{i'} = 1$, and this is a condition that should hold for any element in $\mathrm{Sp}_{\frac{d}{r}}(q^r) = \mathrm{Sp}_2(q^2)$ that is conjugate to g in $\mathrm{Sp}_d(q) = \mathrm{Sp}_4(q)$. Therefore, in (4.8), we need to use only $(1,1) \in \mathcal{S}_2(n(j)) = \mathcal{S}_2(2)$ and

$$\begin{aligned} N(G,H,g) &= \frac{1}{r} \cdot \frac{q^{\frac{1}{2}}rm(j)n(j)^2\rho(V(j),B,g)}{\prod_{i=1}^{r} q^{\frac{1}{2}rm(j)1^2}\bar{\rho}(j,1)} \\ &= \frac{1}{2} \cdot \frac{q^4\rho(V(j),B,g)}{(q\bar{\rho}(j,1))^2} \\ &= \frac{1}{2}q^2 \cdot \frac{(1+\frac{1}{q})(1-\frac{1}{q^2})}{(1-\frac{1}{q^2})} \\ &= \frac{1}{2}q(q+1)\,. \end{aligned}$$

We used equations (4.7) and (4.9) to get the expressions for $\rho(V(j),B,g)$ and $\bar{\rho}(j,1)$. If $\mathcal{K}_j = \{i, l\}$ for some $i, l \in I$ then again, using (4.8),

$$\begin{aligned} N(G,H,g) &\le \frac{1}{2} \sum_{(\bar{n}_1,\bar{n}_2)\in\mathcal{S}_2(2)} \frac{q^4\rho(V(j),B,g)}{q^{\bar{n}_1^2+\bar{n}_2^2}\bar{\rho}(j,\bar{n}_1)(j,\bar{n}_2)} \\ &= \frac{1}{2}\Big(2\frac{\rho(V(j),B,g)}{\bar{\rho}(j,2)} + q^2\frac{\rho(V(j),B,g)}{\bar{\rho}(j,1)^2}\Big) \\ &= \frac{1}{2}\Big(2 + q^2\frac{(1+\frac{1}{q})(1-\frac{1}{q^2})}{(1+\frac{1}{q})^2}\Big) \\ &= \frac{1}{2}\Big(2 + q^2(1-\frac{1}{q})\Big) \\ &= \frac{1}{2}q(q-1)+1 < \frac{1}{2}q(q+1)\,. \end{aligned}$$

This completes the proof. ■

Theorem 4.2.20 *Suppose $G \simeq Sp_d(q)$ and $Sp_{\frac{d}{r}}(q^r) \simeq H < G$ for some prime divisor r of d, and $g \in H$ is a p'-element that is not in the center of G and is not conjugate to any element in $N_G(H) \setminus H$. Furthermore, suppose that $r \neq d$ and $(d,q) \neq (4,3)$.*

(a) *If* $r \neq \frac{d}{2}$ *then* $\mu(G, N_G(H), g) \le q^{-\frac{d}{2}(r-1)}$.

(b) *If* $r = \frac{d}{2}$ *then* $\mu(G, N_G(H), g) \le q^{-\frac{d}{2}(r-1)} \cdot \frac{q}{q-1}$.

Proof: The condition $(d,q) \neq (4,3)$ is to make sure that $N_G(H)$ is a maximal subgroup in G, and hence by Lemma 4.2.1,

$$\mu(G, N_G(H), g) = \frac{N(G, N_G(H), g)}{|G : N_G(H)|} = \frac{N(G, H, g)}{|G : N_G(H)|} \,.$$

Now,

$$\begin{aligned} |G : N_G(H)| &= \frac{1}{r} \cdot \frac{|\mathrm{Sp}_d(q)|}{|\mathrm{Sp}_{\frac{d}{r}}(q^r)|} \\ &= \frac{1}{r} \cdot \frac{q^{\frac{d^2}{2}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)}{q^{\frac{d^2}{2r}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2r}} \left(1 - \frac{1}{q^{2k}}\right)} \\ &= \frac{1}{r} \cdot q^{\frac{d^2}{2}-\frac{d^2}{2r}} \prod_{\substack{1 \le k \le \frac{d}{2} \\ r \nmid k}} \left(1 - \frac{1}{q^{2k}}\right) . \end{aligned}$$

Statement (a) follows from this and Theorem 4.2.19/(a) immediately. If $r = \frac{d}{2}$, then

$$|G : N_G(H)| = \frac{1}{r} q^{2(r^2-r)} \prod_{k=1}^{r-1} \left(1 - \frac{1}{q^{2k}}\right) ,$$

so by Theorem 4.2.19/(b),

$$\begin{aligned} \mu(G, N_G(H), g) &\le q^{-r(r-1)} \prod_{k=1}^{r-1} \frac{\left(1 - \frac{(-1)^k}{q^k}\right)}{\left(1 - \frac{1}{q^{2k}}\right)} \\ &= q^{-r(r-1)} \frac{1}{\prod_{k=1}^{r-1} \left(1 + \frac{(-1)^k}{q^k}\right)} \\ &\le q^{-r(r-1)} \frac{1}{1 - \frac{1}{q}} = q^{-r(r-1)} \frac{q}{q-1} \,. \end{aligned}$$

This completes the proof. ■

Theorem 4.2.21 *Suppose* $G \simeq Sp_d(q)$, $\frac{d}{2} \ge 3$ *odd*, $GU_{\frac{d}{2}}(q^2) \simeq H < G$, *and* $g \in H$ *is a* p'*-element that is not in the center of* G *and is not conjugate to any element in* $N_G(H) \setminus H$. *Then*

$$\mu(G, N_G(H), g) \le q^{-d+2} \,.$$

Proof: As before, we will use (4.8) to obtain an upper bound for $N(G,H,g) = N(G,N_G(H),g)$. Then the upper bound for $\mu(G,N_G(H),g)$ follows immediately, using that

$$\mu(G,N_G(H),g) = \frac{N(G,H,g)}{|G:N_G(H)|}$$

and

$$\begin{aligned}
|G:N_G(H)| &= \frac{1}{2}\cdot\frac{|\mathrm{Sp}_d(q)|}{|\mathrm{GU}_{\frac{d}{2}}(q^2)|} \\
&= \frac{1}{2}\cdot\frac{q^{\frac{d^2}{2}+\frac{d}{2}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{1}{q^{2k}}\right)}{q^{\frac{d^2}{4}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{(-1)^k}{q^k}\right)} \\
&= \frac{1}{2}\cdot q^{\frac{d^2}{4}+\frac{d}{2}}\prod_{k=1}^{\frac{d}{2}}\left(1+\frac{(-1)^k}{q^k}\right).
\end{aligned}$$

Apply the results of Lemmas 4.2.11/(b), 4.2.12/(a) and 4.2.18/(a) to (4.8) with $r=2$ to get

$$N(G,H,g) \le \frac{1}{2}q^{\sum_{i\in\mathcal{A}} m_i^2n_i^2+\sum_{j=1}^{s} m(j)^2n(j)^2+\sum_{i\in I_1} n_i}\,.$$

Here, $\sum_{i\in\mathcal{A}} m_in_i + \sum_{j=1}^{s} m(j)n(j) = \frac{d}{2}$ and if at least two of these summands are non-zero, then

$$\sum_{i\in\mathcal{A}} m_i^2n_i^2 + \sum_{j=1}^{s} m(j)^2n(j)^2 \le \left(\frac{d}{2}-1\right)^2+1 = \frac{d^2}{4}-d+2\,,$$

$$\sum_{i\in\mathcal{A}} m_i^2n_i^2 + \sum_{j=1}^{s} m(j)^2n(j)^2 + \sum_{i\in I_1} n_i \le \frac{d^2}{4}-\frac{d}{2}+2\,.$$

In this case, we handle two sub-cases separately. First, if $\sum_{i\in I_1} n_i < \frac{d}{2}$ then

$$\sum_{i\in\mathcal{A}} m_i^2n_i^2 + \sum_{j=1}^{s} m(j)^2n(j)^2 + \sum_{i\in I_1} n_i \le \frac{d^2}{4}-\frac{d}{2}+1$$

and

$$\mu(G,N_G(H)) \le \frac{q^{\frac{d^2}{4}-\frac{d}{2}+1}}{q^{\frac{d^2}{4}+\frac{d}{2}-1}} = q^{-d+2}\,.$$

And if $\sum_{i\in I_1} n_i = \frac{d}{2}$ then $n_l = 0$ for all $l \notin I_1$, and from (4.8) and Lemma 4.2.11/(b),

$$\begin{aligned} N(G,H,g) &\leq \frac{1}{2}\prod_{i\in I_1}\left[q^{n_i^2+n_i}\prod_{k=1}^{n_i}\left(1-\frac{(-1)^k}{q^k}\right)\right] \\ &\leq q^{\frac{d^2}{4}-\frac{d}{2}+2}\prod_{i\in I_1}\prod_{k=1}^{n_i}\left(1-\frac{(-1)^k}{q^k}\right) \end{aligned}$$

which leads to

$$\mu(G,N_G(H),g) \leq q^{-d+2}\frac{\prod_{i\in I_1}\prod_{k=1}^{n_i}\left(1+\frac{(-1)^k}{q^k}\right)}{\prod_{k=1}^{\frac{d}{2}}\left(1+\frac{(-1)^k}{q^k}\right)} \leq q^{-d+2} .$$

Next, suppose that $\frac{d}{2} = m_i n_i$ for some $i \in \mathcal{A}$. Then $i = i'$ and $m_i \geq 2$ (because g is not a central element in G.) By Lemma 4.2.12/(b),

$$N(G,H,g) \leq \frac{1}{2}q^{\frac{d^2}{4}-\frac{d}{2}} ,$$

which implies

$$\mu(G,N_G(H),g) \leq q^{-d}\cdot\frac{1}{\prod_{k=1}^{\frac{d}{2}}\left(1+\frac{(-1)^k}{q^k}\right)} < q^{-d+1} .$$

Finally, if $\frac{d}{2} = m(j)n(j)$ for some $1 \leq j \leq s$ then by Lemma 4.2.17/(b),

$$N(G,H,g) \leq \frac{1}{2}q^{\frac{d^2}{4}-\frac{d}{2}}$$

and like in the previous case, that implies $\mu(G,N_G(H),g) \leq q^{-d+1}$. ■

4.3 Case II: p'-Elements Acting Non-Trivially on an Extension Field

Throughout this section, d is a positive integer, r is a prime divisor of d and q is a prime power such that $\gcd(r,q) = 1$.

Lemma 4.3.1 *Let $G = GL_d(q)$, $GL_{\frac{d}{r}}(q^r) \simeq H < G$ and $g \in N_G(H) \setminus H$ such that $g^r = \lambda I$ for some $\lambda \in \mathbf{F}_q$. Then the characteristic polynomial of g in G is*

$$\chi_g(x) = (x^r - \lambda)^{\frac{d}{r}} .$$

Proof: Let a be the multiplicative order of q modulo r (so $1 \leq a \leq r-1$), let $T = \mathrm{GL}_{da}(q)$ and $Y < X < T$ with $Y \simeq \mathrm{GL}_{\frac{d}{r}}(q^{ar})$ and $X \simeq \mathrm{GL}_d(q^a)$. By Lemma 2-2-4, $N_T(Y) \simeq Z_{ar} \ltimes Y$, $N_X(Y) \simeq Z_a \ltimes X$ and $N_X(Y) \simeq Z_r \ltimes Y$. Since $\gcd(a,r) = 1$, $Z_{ar} \simeq Z_a \times Z_r$ and there are cyclic subgroups $A \simeq Z_a$ and $R \simeq Z_r$ such that

$$N_X(Y) = R \ltimes Y \ , \ N_T(X) = A \ltimes X \ \text{ and } \ N_T(Y) = (A \times R) \ltimes Y \ .$$

We may identify G with $C_X(A) \simeq \mathrm{GL}_d(q)$ and H with $C_Y(A) \simeq \mathrm{GL}_{\frac{d}{r}}(q^r)$. Notice that R normalizes H, since for any $a \in A, r \in R$ and $h \in H$, $h^{ra} = h^{ar} = h^r$ showing that h^r is an element of Y that is centralized by a and thus $h^r \in H$. Also, since $R \leq X \cap C(A) = G$ but $R \cap H \leq R \cap Y = \{1\}$, we have that

$$N_G(H) = R \ltimes H \ .$$

Next, let $\mu \in Z(X) \simeq \mathbf{F}_{q^a}$ be an r^{th} root of unity, and consider the norm map N from $Z(Y) \simeq \mathbf{F}_{q^{ar}}$ to $Z(H) \simeq \mathbf{F}_{q^r}$. Since $g \in R \ltimes H \setminus H \subseteq R \ltimes Y \setminus Y$,

$$N(\alpha) = \alpha \cdot \alpha^{q^a} \cdot \ldots \cdot \alpha^{q^{a(r-1)}} = \alpha \cdot \alpha^g \cdot \ldots \cdot \alpha^{g^{r-1}}$$

for any $x \in Z(Y)$. Clearly,

$$N(\mu) = \mu \cdot \mu^{q^a} \cdot \ldots \cdot \mu^{q^{a(r-1)}} = \mu^r = 1 \ ,$$

hence by Hilbert's Theorem 90, $\mu = \nu^g \nu^{-1}$ for some $\nu \in Z(Y)$. Then

$$\nu g \nu^{-1} = g \nu^g \nu^{-1} = g\mu$$

showing that g is conjugate to $g\mu$ in $R \ltimes Y$, hence g is conjugate to $g\mu$ in $X \simeq \mathrm{GL}_d(q^a)$.

This implies that the r^{th} roots of λ are all eigenvalues of g with the same multiplicity, therefore the characteristic polynomial of g has to be a power of the polynomial $x^r - \lambda$. ∎

Lemma 4.3.2 *Let $G = GL_d(q)$, $GL_{\frac{d}{r}}(q^r) \simeq H < G$ and $g \in N_G(H) \setminus H$ such that $g^r = \lambda I$ for some $\lambda \in \mathbf{F}_q$. Then*

$$|C_G(g)| \leq q^{\frac{d^2}{r}} \prod_{k=1}^{\frac{d}{r}} \left(1 - \frac{1}{q^{rk}}\right) .$$

Proof: Identify G with $\mathrm{GL}(V)$ for a vector space V of dimension d over $\mathbf{F}_q$, and recall the notations we used in Section 3.5. That is, Let o be the order of g (which divides $r(q-1)$ and hence it is coprime to q); let $x^o - 1 = \prod_{i=1}^{t} f_i(x)$ be the factorization of the polynomial $x^o - 1$ into irreducible factors over $\mathbf{F}_q$, and for each $1 \leq i \leq t$, let m_i be the degree of $f_i(x)$, $V_i = \{v \in V \,|\, v f_i(x) = 0\}$ and $\dim_{\mathbf{F}_q}(V_i) = m_i n_i$. Then

$$|C_G(g)| = \prod_{i=1}^{t} |\mathrm{GL}_{n_i}(q^{m_i})| = q^{\sum_{i=1}^{t} m_i n_i^2} \prod_{i=1}^{t} \prod_{k=1}^{n_i} \left(1 - \frac{1}{q^{m_i k}}\right) .$$

By the previous lemma, the characteristic polynomial of g is $(x^r - \lambda)^{\frac{d}{r}}$, therefore

$$n_i = \begin{cases} \frac{d}{r} & \text{if } f_i(x) \text{ divides } x^r - \lambda \, ; \\ 0 & \text{otherwise,} \end{cases}$$

and obviously $\{i \,|\, n_i \neq 0\} \leq r$ and $\sum_{i, n_i \neq 0} m_i = r$. This implies

$$\begin{aligned} q^{\sum_{i=1}^{t} m_i n_i^2} \prod_{i=1}^{t} \prod_{k=1}^{n_i} \left(1 - \frac{1}{q^{m_i k}}\right) &= q^{\frac{d^2}{r}} \prod_{i, n_i \neq 0} \prod_{k=1}^{\frac{d}{r}} \left(1 - \frac{1}{q^{m_i k}}\right) \\ &= q^{\frac{d^2}{r}} \prod_{k=1}^{\frac{d}{r}} \prod_{i, n_i \neq 0} \left(1 - \frac{1}{q^{m_i k}}\right) \\ &\leq q^{\frac{d^2}{r}} \prod_{k=1}^{\frac{d}{r}} \left(1 - \frac{1}{q^{rk}}\right) , \end{aligned}$$

as we wanted. ■

Lemma 4.3.3 *Let $G = Sp_d(q)$, q an odd prime power, $Sp_{\frac{d}{r}}(q^r) \simeq H < G$ and $g \in N_G(H) \setminus H$ such that $g^r = \lambda I$ with $\lambda = 1$ or $\lambda = -1$. Furthermore, assume that* *q is odd.*

(a) *If* $r = 2$ *and* $\lambda = 1$ *then* $|C_G(g)| = q^{\frac{d^2}{4}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right)^2$.

(b) *If* $r = 2$ *and* $\lambda = -1$ *then* $|C_G(g)| \leq q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{(-1)^k}{q^k}\right)$.

(c) *If* $r \geq 3$ *then* $|C_G(g)| \leq q^{\frac{d^2+d}{2r}} \left(1 + \frac{1}{q}\right)^{r-1}$.

Proof: Keeping the notations of the previous lemma, by Theorem 3.5.19,

$$|C_G(g)| = q^{\frac{1}{2}\sum\limits_{i=1}^{t} m_i n_i^2} \cdot \prod_{i=1}^{t} \rho(V_i, g)$$

where

$$\rho(V_i, g) = \begin{cases} q^{\frac{n_i}{2}} \prod_{k=1}^{\frac{n_i}{2}} \left(1 - \frac{1}{q^{2k}}\right) & \text{if } i \in I_1 \,; \\ \prod_{k=1}^{n_i} \left(1 - \frac{(-1)^k}{q^{\frac{1}{2}m_i k}}\right) & \text{if } i \in I_2 \,; \\ \left[\prod_{k=1}^{n_i} \left(1 - \frac{1}{q^{m_i k}}\right)\right]^{\frac{1}{2}} & \text{if } i \in J \,. \end{cases}$$

Again, the characteristic polynomial of g is $(x^r - \lambda)^{\frac{d}{r}}$ and this implies

$$n_i = \begin{cases} \frac{d}{r} & \text{if } f_i(x) \text{ divides } x^r - \lambda \,; \\ 0 & \text{otherwise}\,, \end{cases}$$

$\sum_{i, n_i \neq 0} m_i = r$, and the exponent of q in the formula for $|C_G(g)|$, $\frac{1}{2}\sum\limits_{i=1}^{t} m_i n_i^2$ is equal to $\frac{d^2}{r}$.

If $r = 2$ and $\lambda = 1$ then $x^r - \lambda = x^2 - 1 = (x+1)(x-1) = \prod_{i \in I_1} f_i(x)$ and

$$\begin{aligned} |C_G(g)| &= q^{\frac{d^2}{4}} \prod_{i \in I_1} \rho(V_i, g) \\ &= q^{\frac{d^2}{4}+\frac{d}{2}} \prod_{i \in I_1} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right) \\ &= q^{\frac{d^2}{4}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right)^2 . \end{aligned}$$

If $r = 2$ and $\lambda = -1$ then $x^r - \lambda = x^2 + 1$ and either $x^2 + 1 = f_l(x)$ for some $l \in I_2$ or $x^2 + 1 = f_l(x) f_{l'}(x)$ for some $l \in J$. In the first case,

$$|C_G(g)| = q^{\frac{d^2}{4}} \rho(V_l, g) = q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{(-1)^k}{q^k}\right)$$

and in the second case

$$|C_G(g)| = q^{\frac{d^2}{4}}\rho(V_l,g)\rho(V_{l'},g) = q^{\frac{d^2}{4}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{1}{q^k}\right).$$

Finally, if r is an odd prime number then either $x+1$ or $x-1$ divides $x^r-\lambda$, in other words there is exactly one $i \in I_1$ with $f_i(x)$ dividing the characteristic polynomial of g. For this i, $\rho(V_i,g) < q^{\frac{n_i}{2}} = q^{\frac{d}{2r}}$, and for any $i \neq I_1$, $\rho(V_i,g) < 1+\frac{1}{q}$. This implies (c). ■

Lemma 4.3.4 *Let $G = Sp_d(q)$, q an odd prime power, $\frac{d}{2}$ an odd number, $GU_{\frac{d}{2}}(q^2) \simeq H < G$ and $g \in N_G(H) \setminus H$ such that $g^2 \in Z(G)$. Then $g^2 = -I$ and*

$$|C_G(g)| \leq q^{\frac{d^2}{4}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{(-1)^k}{q^k}\right).$$

Proof: Keep the notations of the previous two lemmas. Again, n_i is either $\frac{d}{2}$ or 0 for all i. In particular, since in general, n_i is even for all $i \in I_1 = \{i \mid f_i(x) = x \pm 1\}$, this forces n_i to be zero for any $i \in I_1$. In other words the characteristic polynomial of g is not divisible by $x+1$ or $x-1$, and hence $g^2 = -I$. The rest follows like part (b) of the previous lemma. ■

Definition 4.3.5 *For any $\alpha \in \mathbf{F}_q^*$, define the set $\mathcal{S}(\alpha)$ as follows. First, let σ be the Frobenius action on $GL_{\frac{d}{r}}(q^r)$, that sends a matrix (a_{ij}) to (a_{ij}^q). Then let*

$$\mathcal{S}(\alpha) = \{N \in GL_{\frac{d}{r}}(q^r) \mid N^{\sigma^{r-1}} \cdot N^{\sigma^{r-2}} \cdot \ldots \cdot N^{\sigma} \cdot N = \alpha I\}.$$

Lemma 4.3.6 *For any $\alpha \in \mathbf{F}_q^*$,*

$$|\mathcal{S}(\alpha)| = \frac{|GL_{\frac{d}{r}}(q^r)|}{|GL_{\frac{d}{r}}(q)|}.$$

Proof: Since the norm function from $\mathbf{F}_{q^r}^*$ to $\mathbf{F}_q^*$ is surjective, $|\mathcal{S}(\alpha)| = |\mathcal{S}(1)|$ for any $\alpha \in \mathbf{F}_q^*$.

Suppose that $N \in \mathrm{GL}_{\frac{d}{r}}(q^r)$ and $N^{\sigma^{r-1}} \cdot \ldots \cdot N^\sigma \cdot N = I$. By Lang's Theorem, there is a $\frac{d}{r} \times \frac{d}{r}$-matrix T over the algebraic closure of $\mathbf{F}_{q^r}$ such that $T^\sigma T^{-1} = N$. Then

$$T^{\sigma^r} \cdot T^{-1} = (T^\sigma T^{-1})^{\sigma^{r-1}} \cdot \ldots \cdot (T^\sigma T^{-1})^\sigma \cdot (T^\sigma T^{-1}) = I$$

and this means that actually T is in $\mathrm{GL}_{\frac{d}{r}}(q^r)$. This shows that every element in $\mathcal{S}(1)$ can be written as $T^\sigma T^{-1}$ with some $T \in \mathrm{GL}_{\frac{d}{r}}(q^r)$. On the other hand, if $T^\sigma T^{-1} = S^\sigma S^{-1}$ for $T, S \in \mathrm{GL}_{\frac{d}{r}}(q^r)$ then $(S^{-1}T)^\sigma = S^{-1}T$, that is, $S^{-1}T \in \mathrm{GL}_{\frac{d}{r}}(q)$. ∎

Lemma 4.3.7 *If $\frac{d}{r}$ is even then*

$$|\mathcal{S}(1) \cap Sp_{\frac{d}{r}}(q^r)| = |\mathcal{S}(-1) \cap Sp_{\frac{d}{r}}(q^r)| = \frac{|Sp_{\frac{d}{r}}(q^r)|}{|Sp_{\frac{d}{r}}(q)|}.$$

Proof: For $\mathcal{S}(1) \cap \mathrm{Sp}_{\frac{d}{r}}(q^r)$, or if r odd then for $\mathcal{S}(-1) \cap \mathrm{Sp}_{\frac{d}{r}}(q^r)$ the proof goes exactly the same way as the proof of the previous lemma. For $\mathcal{S}(-1) \cap \mathrm{Sp}_{\frac{d}{2}}(q^2)$, it is slightly different, because in this case $\mathcal{S}(-1) \cap \mathrm{Sp}_{\frac{d}{2}}(q^2)$ cannot be obtained from $\mathcal{S}(1) \cap \mathrm{Sp}_{\frac{d}{2}}(q^2)$ by multiplying its elements with a certain scalar matrix.

Suppose that $\frac{d}{2}$ is even, $N \in \mathrm{Sp}_{\frac{d}{2}}(q^2)$ and $N^\sigma \cdot N = -I$. By Lang's Theorem, there is a symplectic $\frac{d}{r} \times \frac{d}{r}$-matrix T over the algebraic closure of $\mathbf{F}_{q^2}$ such that $T^\sigma T^{-1} = N$. Then

$$T^{\sigma^2} \cdot T^{-1} = (T^\sigma T^{-1})^\sigma \cdot (T^\sigma T^{-1}) = -I$$

and this means that for every entry α in T, $\alpha^{q^2-1} = -1$. Fix an element μ in $\mathbf{F}_{q^4}$ such that $\mu^{q^2-1} = -1$ and let $M \in \mathrm{Sp}_{\frac{d}{2}}(q^4)$ be the diagonal matrix having μ and μ^{-1} both $\frac{d}{4}$ times in its diagonal. Then MT is a symplectic matrix over $\mathbf{F}_{q^2}$ and hence $T \in M^{-1} \cdot \mathrm{Sp}_{\frac{d}{2}}(q^2) = M \cdot \mathrm{Sp}_{\frac{d}{2}}(q^2)$. This shows that every element in $\mathcal{S}(-1)$ can be written as $(MA)^\sigma (MA)^{-1}$ with some $A \in \mathrm{Sp}_{\frac{d}{2}}(q^2)$. On the other hand, if $(MA)^\sigma(MA)^{-1} = (MB)^\sigma(MB)^{-1}$ for $A, B \in \mathrm{Sp}_{\frac{d}{2}}(q^2)$ then $A^\sigma A^{-1} = B^\sigma B^{-1}$, $(B^{-1}A)^\sigma = B^{-1}A$ and $B^{-1}A \in \mathrm{Sp}_{\frac{d}{2}}(q)$. ■

Lemma 4.3.8 *Let $G = GL_d(q)$, $GL_{\frac{d}{r}}(q^r) \simeq H < G$ and $\alpha \in \mathbf{F}_q^*$. Then*

$$|\{g \in N_G(H) \setminus H \mid g^r = \alpha I\}| \leq (r-1) \cdot \frac{|GL_{\frac{d}{r}}(q^r)|}{|GL_{\frac{d}{r}}(q)|} .$$

Proof: Identify $N_G(H)$ with $\langle\sigma\rangle \ltimes \mathrm{GL}_{\frac{d}{r}}(q^r)$ and it is enough to show that for each $1 \leq k \leq r-1$,

$$|\{g \in \sigma^k \cdot \mathrm{GL}_{\frac{d}{r}}(q^r) \,|\, g^r = \alpha I\}| \leq \frac{|\mathrm{GL}_{\frac{d}{r}}(q^r)|}{|\mathrm{GL}_{\frac{d}{r}}(q)|} .$$

This is true for $k = 1$ by the previous lemma, because if $g = \sigma \cdot M$ for some $M \in \mathrm{GL}_{\frac{d}{r}}(q^r)$, then $g^r = \alpha I$ is equivalent to $M^{\sigma^{r-1}} \cdot \ldots \cdot M^\sigma \cdot M = \alpha I$. Now suppose $k > 1$ and let $1 < l \leq r-1$ such that $kl \equiv 1 \pmod r$. Then $g \in \sigma^k \cdot \mathrm{GL}_{\frac{d}{r}}(q^r)$ and $g^r = \alpha I$ implies $g^l \in \sigma \cdot \mathrm{GL}_{\frac{d}{r}}(q^r)$ and $(g^l)^r = \alpha^l I$. Furthermore, if h is also in $\sigma^k \cdot \mathrm{GL}_{\frac{d}{r}}(q^r)$ and $h^r = \alpha I$, then $h^l = g^l$ would imply $h = g$ (because we already have $h^r = g^r$ and $(r; l) = 1$). Therefore

$$|\{g \in \sigma^k \cdot \mathrm{GL}_{\frac{d}{r}}(q^r) \,|\, g^r = \alpha I\}| \;\leq\; |\{g \in \sigma \cdot \mathrm{GL}_{\frac{d}{r}}(q^r) \,|\, g^r = \alpha^l I\}| . \quad ■$$

Lemma 4.3.9 *Let $G = Sp_d(q)$, q an odd prime power, $\frac{d}{r}$ even, $Sp_{\frac{d}{r}}(q^r) \simeq H < G$ and $\alpha = \pm 1$. Then*

$$|\{g \in N_G(H) \setminus H \mid g^r = \alpha I\}| = \frac{|Sp_{\frac{d}{r}}(q^r)|}{|Sp_{\frac{d}{r}}(q)|} .$$

Proof: This is true simply because $N_G(H) \simeq \langle\sigma\rangle \ltimes \mathrm{Sp}_{\frac{d}{r}}(q^r)$ and $(\sigma M)^r = \alpha I$ if and only if $M \in \mathcal{S}(\alpha)$. And the number of such matrices M is given in Lemma 4.3.7. ■

Lemma 4.3.10 *Let $G = Sp_d(q)$, q an odd prime power, $\frac{d}{2}$ odd and $GU_{\frac{d}{2}}(q^2) \simeq H < G$. Then*

$$\{g \in N_G(H) \setminus H \mid g^2 = -I\}| = \frac{|GU_{\frac{d}{2}(q^2)}|}{|O_{\frac{d}{2}}(q)|} .$$

Proof: If we identify H with the set of $\frac{d}{2} \times \frac{d}{2}$ unitary matrices over $\mathbf{F}_{q^2}$ then there is an element $\alpha \in N_G(H) \setminus H$ such that $\alpha^2 = -I$ and $(a_{ij})^\alpha = (a_{ij}^q)$ for every matrix (a_{ij}) in H. Now for $N \in H$,

$$(\alpha N)^2 = -I \Longleftrightarrow \alpha N \alpha N = -I \Longleftrightarrow N^\alpha N = I .$$

As in the GL and Sp cases, every $N \in H$ can be written as $T^\sigma T^{-1}$ for some unitary matrix T over the algebraic closure of $\mathbf{F}_{q^2}$, and $N^\alpha N = N^\sigma N = I$ if and only if $T \in \mathrm{GU}_{\frac{d}{2}}(q^2)$. On the other hand, if $T, S \in \mathrm{GU}_{\frac{d}{2}}(q^2)$ and $T^\sigma T^{-1} = S^\sigma S^{-1}$ then $(S^{-1}T)^\sigma = S^{-1}T$, that is, all the entries of $S^{-1}T$ are in $\mathbf{F}_q$ and hence $S^{-1}T$ is a matrix in $\mathrm{GL}_{\frac{d}{2}}(q)$ that is equal to the inverse of its transpose matrix. ∎

Lemma 4.3.11 *Let $G = GL_6(q)$, $GL_2(q^3) \simeq H < G$ and $\alpha \in \mathbf{F}_q^*$. Furthermore, assume that $(q;3) = 1$. Then*

$$|\{g \in H \mid g^3 = \alpha I\}| = \begin{cases} 0 & \textit{if } x^3 - \alpha \textit{ is irreducible over } \mathbf{F}_{q^3} \ ; \\ q^6 - q^3 + 1 & \textit{if } x^3 - \alpha \textit{ has one root in } \mathbf{F}_{q^3} \ ; \\ 3(q^6 + q^3 + 1) & \textit{if } x^3 - \alpha \textit{ has three roots in } \mathbf{F}_{q^3} \ . \end{cases}$$

Proof: If $g \in \mathrm{GL}_2(q^3)$ then the characteristic polynomial of g is a second degree polynomial such that it either divides $x^3 - \alpha$ or has a double root that is also a root of $x^3 - \alpha$. Therefore $x^3 - \alpha$ cannot be irreducible over $\mathbf{F}_{q^3}$.

Suppose $x^3 - \alpha = f_1(x) \cdot f_2(x)$ with $f_1(x)$ linear and $f_2(x)$ irreducible quadratic. Then there are two conjugacy classes in H of the elements g with $g^3 = \alpha I$, one conjugacy class with characteristic polynomial $f_1(x)^2$ and an other one with characteristic polynomial $f_2(x)$. Therefore

$$|\{g \in H \mid g^3 = \alpha I\}| = 1 + \frac{|H|}{q^6 - 1} = 1 + \frac{(q^6-1)(q^6-q^3)}{q^6-1} = q^6 - q^3 + 1 .$$

Now suppose $x^3-\alpha=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ with $\alpha_1,\alpha_2,\alpha_3\in\mathbf{F}_{q^3}$. Then there are six conjugacy classes of the elements g in H with $g^3=\alpha I$, since the characteristic polynomial of such a g can be either $(x-\alpha_i)^2$ for some i or $(x-\alpha_i)(x-\alpha_j)$ with $i\neq j$. And it follows that

$$|\{g\in H\mid g^3=\alpha I\}|=3+3\frac{|H|}{(q^3-1)^2}=3+3q^3(q^3+1)=3(q^6+q^3+1)\ ,$$

as we stated. ■

Lemma 4.3.12 *Let* $G=GL_d(q)$, $GL_{\frac{d}{r}}(q^r)\simeq H<G$, r *an odd prime divisor of* d *(not equal to* d*) and* $g\in N_G(H)\setminus H$ *such that* $g^r\in Z(G)$. *Then*

$$\mu(G,N_G(H),g)<\frac{1}{q^{d(r-1)}}\ .$$

Proof: By Lemma 4.1.2,

$$\mu(G,N_G(H),g)=\frac{|C_G(g)|\cdot|\mathcal{C}(G,N_G(H),g)|}{|G|}\ .$$

Here,

$$|G|=|\mathrm{GL}_d(q)|=q^{d^2}\prod_{k=1}^{d}\left(1-\frac{1}{q^k}\right)\ ,$$

$$|\mathcal{C}(G,N_G(H),g)|<|N_G(H)|=r\cdot q^{\frac{d^2}{r}}\prod_{k=1}^{\frac{d}{r}}\left(1-\frac{1}{q^{rk}}\right)\ ,$$

and by Lemma 4.3.2,

$$|C_G(g)|\leq q^{\frac{d^2}{r}}\prod_{k=1}^{\frac{d}{r}}\left(1-\frac{1}{q^{rk}}\right)\ .$$

Therefore,

$$\mu(G,N_G(H),g)<q^{\frac{2}{r}d^2-d^2}\cdot r\cdot\frac{\prod_{k=1}^{\frac{d}{r}}\left(1-\frac{1}{q^{rk}}\right)^2}{\prod_{k=1}^{d}\left(1-\frac{1}{q^k}\right)}\ .$$

Notice that (by using Lemma 4.1.4)

$$r\cdot\frac{\prod_{k=1}^{\frac{d}{r}}\left(1-\frac{1}{q^{rk}}\right)^2}{\prod_{k=1}^{d}\left(1-\frac{1}{q^k}\right)}<r\cdot\frac{1}{\frac{1}{4}}=4r<q^{2r}\ ,$$

therefore

$$\mu(G, N_G(H), g) < q^{\frac{2}{r}d^2 - d^2 + 2r}$$

and the statement of this lemma follows whenever

$$\frac{2-r}{r}d^2 + 2r \leq -d(r-1)\ ,$$

or equivalently,

$$dr(r-1) + 2r^2 \leq d^2(r-2)\ .$$

Since $d = nr$ for some integer n with $n \geq 2$, we can rewrite this inequality as

$$nr^2(r-1) + 2r^2 \leq n^2r^2(r-1)\ ;$$

$$n(r-1) + 2 \leq n^2(r-2)\ ;$$

$$n\frac{r-1}{r-2} + \frac{2}{r-2} \leq n^2\ .$$

Now if $r \geq 5$ then

$$n\frac{r-1}{r-2} + \frac{2}{r-2} \leq \frac{4n}{3} + \frac{2}{3} \leq \frac{2n^2}{3} + \frac{n}{3} < n^2$$

for any $n \geq 2$, and if $r = 3$ then

$$n\frac{r-1}{r-2} + \frac{2}{r-2} = 2n + 2 < n^2$$

whenever $n \geq 3$. This proves the lemma except for the case $d = 6$, $r = 3$. We will handle this case by giving a more careful upper bound for $|\mathcal{C}(G, N_G(H), g)|$.

From now, suppose that $d = 6$ and $r = 3$. Notice that then q is not a power of 3. Since $g^3 = \alpha I$ for some $\alpha \in \mathbf{F}_q^*$, clearly

$$\mathcal{C}(G, N_G(H), g) \subseteq \{h \in N_G(H) \mid h^3 = \alpha I\}\ .$$

By Lemmas 4.3.8 and 4.3.11,

$$\begin{aligned}
|\{h \in N_G(H) \mid h^3 = \alpha I\}| &\leq 2\frac{|\mathrm{GL}_2(q^3)|}{|\mathrm{GL}_2(q)|} + 3(q^6 + q^3 + 1) \\
&= 2\frac{q^3(q^3-1)(q^6-1)}{q(q-1)(q^2-1)} + 3(q^6 + q^3 + 1) \\
&= 2q^2(q^2+q+1)(q^4+q^2+1) + 3(q^6 + q^3 + 1) \\
&= 2q^8 + 2q^7 + 7q^6 + 2q^5 + 4q^4 + 5q^3 + 2q^2 + 3\ .
\end{aligned}$$

If $q \geq 4$ then this is less then $3q^8$, so $|\mathcal{C}(G, N_G(H), g)| < 3q^8$ and

$$\begin{aligned}
\mu(G, N(G), g) &\leq \frac{|C_G(g)| \cdot 3q^8}{|G|} \\
&\leq \frac{q^{12} \prod_{k=1}^{2} \left(1 - \frac{1}{q^{3k}}\right) \cdot 3q^8}{q^{36} \prod_{k=1}^{6} \left(1 - \frac{1}{q^k}\right)} \\
&\leq q^{-16} \cdot 3 \cdot \frac{q-1}{q-2} \\
&\leq q^{-16} \cdot 3 \cdot \frac{3}{2} \\
&< q^{-14} < q^{-12} = q^{-d(r-1)} ,
\end{aligned}$$

If $q = 2$ then using the fact that in $\mathbf{F}_8$ every polynomial of the form $x^3 - \alpha$ has exactly one root, by Lemma 4.3.11,

$$|\{h \in H \mid h^3 = \alpha I\}| = q^6 - q^3 + 1 = 64 - 8 + 1 = 57 ,$$

and then

$$|\mathcal{C}(G, N_G(H), g)| \leq 2 \frac{|\mathrm{GL}_2(8)|}{|\mathrm{GL}_2(2)|} + 57 = 2 \cdot \frac{3528}{6} + 57 = 1233 ,$$

$$\begin{aligned}
\mu(G, N(G), g) &\leq \frac{|C_G(g)| \cdot 1233}{|G|} \\
&\leq \frac{2^{12} \prod_{k=1}^{2} \left(1 - \frac{1}{8^k}\right) \cdot 1233}{2^{36} \prod_{k=1}^{6} \left(1 - \frac{1}{2^k}\right)} \\
&= \frac{1233}{2^{24}\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{32}\right)} \\
&= \frac{1233}{2^{12} \cdot 1395} \\
&< 2^{-12} = q^{-d(r-1)} .
\end{aligned}$$

This completes the proof. ∎

Lemma 4.3.13 *Let* $G = GL_d(q)$, *q odd,* $d \geq 4$ *even,* $GL_{\frac{d}{2}}(q^2) \simeq H < G$ *and* $g \in N_G(H) \setminus H$ *such that* $g^2 \in Z(G)$.

(a) *If* $d \geq 6$ *then* $\mu(G, N_G(H), g) < \frac{1}{q^d}$.

(b) *If* $d = 4$ *and* $q \geq 5$ *then* $\mu(G, N_G(H), g) < \frac{3}{q^4}$.

(c) *If* $d = 4$ *and* $q = 3$ *then* $\mu(G, N_G(H), g) < \frac{1}{19}$.

Proof: First, let $g^2 = \alpha I$ and we will find an upper bound for the cardinality of the set $\{h \in H \mid h^2 = \alpha I\}$. Assume that h is en element of $\mathrm{GL}_{\frac{d}{2}}(q^2)$ with $h^2 = \alpha I$. Then there is an element $\lambda \in \mathbf{F}_{q^2}$ such that $\lambda^2 = \alpha$ and the characteristic polynomial of h is equal to $(x-\lambda)^l(x+\lambda)^{\frac{d}{2}-l}$ for some integer l between 0 and $\frac{d}{2}$. Then the order of the centralizer of h in $\mathrm{GL}_{\frac{d}{2}}(q^2)$ is $|\mathrm{GL}_l(q^2)| \cdot |\mathrm{GL}_{\frac{d}{2}-l}(q^2)|$ and the cardinality of the conjugacy class of h is

$$
\begin{aligned}
\frac{|GL_{\frac{d}{2}}(q^2)|}{|\mathrm{GL}_l(q^2)| \cdot |\mathrm{GL}_{\frac{d}{2}-l}(q^2)|} &= \frac{q^{\frac{d^2}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)}{q^{2l^2 + 2(\frac{d}{2}-l)^2} \prod_{k=1}^{l} \left(1 - \frac{1}{q^{2k}}\right) \prod_{k=1}^{\frac{d}{2}-l} \left(1 - \frac{1}{q^{2k}}\right)} \\
&= q^{2dl - 4l^2} \cdot \frac{\prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)}{\prod_{k=1}^{l} \left(1 - \frac{1}{q^{2k}}\right) \prod_{k=1}^{\frac{d}{2}-l} \left(1 - \frac{1}{q^{2k}}\right)} \\
&< q^{2dl - 4l^2} \frac{1}{\prod_{k=1}^{\infty} \left(1 - \frac{1}{q^{2k}}\right)} \\
&< q^{2l(d-2l)} \frac{q^2 - 1}{q^2 - 2} \\
&\leq \frac{8}{7} \cdot q^{2l(d-2l)} .
\end{aligned}
$$

Since l characterizes the conjugacy class of h in $\mathrm{GL}_{\frac{d}{2}}(q^2)$, we have

$$\begin{aligned}
|\{h \in H \mid h^2 = \alpha I\}| &< \sum_{l=0}^{\frac{d}{2}} \frac{8}{7} q^{2l(d-2l)} \\
&\le \frac{8}{7} \cdot 2 \sum_{l=0}^{\lfloor \frac{d}{4} \rfloor} q^{2l(d-2l)} \\
&\le \frac{16}{7} \sum_{k=0}^{\lfloor \frac{d^2}{4} \rfloor} q^k \\
&= \frac{16}{7(q-1)} (q^{\lfloor \frac{d^2}{4} \rfloor + 1} - 1) \\
&< \frac{16}{14} \cdot q^{\frac{d^2}{4}+1} .
\end{aligned}$$

This together with Lemma 4.3.8 imply that

$$\begin{aligned}
|\mathcal{C}(G, N_G(H), g)| &< \frac{|\mathrm{GL}_{\frac{d}{2}}(q^2)|}{|\mathrm{GL}_{\frac{d}{2}}(q)|} + \frac{16}{14} \cdot q^{\frac{d^2}{4}+1} \\
&= \frac{q^{\frac{d^2}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)}{q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{k}}\right)} + \frac{16}{14} \cdot q^{\frac{d^2}{4}+1} \\
&< q^{\frac{d^2}{4}} \cdot \frac{q-1}{q-2} + \frac{16}{14} \cdot q^{\frac{d^2}{4}+1} \\
&= q^{\frac{d^2}{4}+1} \left(\frac{q-1}{q(q-2)} + \frac{16}{14}\right) \\
&\le q^{\frac{d^2}{4}+1} \left(\frac{2}{3} + \frac{16}{14}\right) \\
&< 2 \cdot q^{\frac{d^2}{4}+1} .
\end{aligned}$$

For $d = 4$ we will need a little more careful upper bound:

$$\begin{aligned}
|\{h \in H \mid h^2 = \alpha I\}| &= \sum_{l=0}^{2} \frac{|\mathrm{GL}_2(q^2)|}{|\mathrm{GL}_l(q^2)| \cdot |\mathrm{GL}_{2-l}(q^2)|} \\
&= 2 + \frac{q^2(q^2-1)(q^4-1)}{(q^2-1)(q^2-1)} \\
&= q^4 + q^2 + 2 ;
\end{aligned}$$

$$\begin{aligned}
|\mathcal{C}(G, N_G(H), g)| &\leq \frac{|\mathrm{GL}_2(q^2)|}{|\mathrm{GL}_2(q)|} + q^4 + q^2 + 2 \\
&= \frac{q^2(q^2-1)(q^4-1)}{q(q-1)(q^2-1)} + q^4 + q^2 + 2 \\
&= 2q^4 + q^3 + 2q^2 + q + 2 \\
&\leq q^4\big(2 + \frac{1}{3} + \frac{2}{9} + \frac{1}{27} + \frac{2}{81}\big) = q^4 \cdot \frac{162 + 27 + 18 + 3 + 2}{81} \\
&= \frac{212}{81} \cdot q^4 .
\end{aligned}$$

And if $q \geq 5$ then

$$\begin{aligned}
|\mathcal{C}(G, N_G(H), g)| &\leq q^4\big(2 + \frac{1}{5} + \frac{2}{25} + \frac{1}{125} + \frac{2}{625}\big) \\
&= q^4\big(2 + \frac{125 + 50 + 5 + 2}{625}\big) = q^4\big(2 + \frac{182}{625}\big) \\
&< \frac{23}{10} \cdot q^4 .
\end{aligned}$$

After this, use the formula given by Lemma 4.1.2:

$$\mu(G, N_G(H), g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H), g)|}{|G|} .$$

Here,

$$|G| = |\mathrm{GL}_d(q)| = q^{d^2} \prod_{k=1}^{d} \Big(1 - \frac{1}{q^k}\Big)$$

and from Lemma 4.3.2,

$$|C_G(g)| \leq q^{\frac{d^2}{2}} \prod_{k=1}^{\frac{d}{2}} \Big(1 - \frac{1}{q^{2k}}\Big) < q^{\frac{d^2}{2}} .$$

So if $d \geq 6$ then

$$\begin{aligned}
\mu(G, N_G(H), g) &\leq \frac{q^{\frac{d^2}{2}} \cdot 2q^{\frac{d^2}{4}+1}}{q^{d^2} \prod_{k=1}^{d} \big(1 - \frac{1}{q^k}\big)} \\
&< \frac{2q^{\frac{3}{4}d^2+1}}{\frac{1}{4}q^{d^2}} \\
&= 8q^{-\frac{d^2}{4}+1} < q^{-\frac{d^2}{4}+3} \\
&\leq q^{-d} ;
\end{aligned}$$

if $d = 4$ and $q \geq 5$ then

$$\begin{aligned}
\mu(G, N_G(H), g) &< \frac{q^8 \prod_{k=1}^{2} \left(1 - \frac{1}{q^{2k}}\right) \cdot \frac{23}{10} q^4}{q^{16} \prod_{k=1}^{4} \left(1 - \frac{1}{q^k}\right)} \\
&= \frac{\frac{23}{10} q^{12}}{q^{16}\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^3}\right)} \\
&\leq q^{-4} \cdot \frac{23}{10} \cdot \frac{5}{4} \cdot \frac{125}{124} = q^{-4} \cdot \frac{2875}{992} \\
&< 3 \cdot q^{-4} \, ;
\end{aligned}$$

and finally, if $d = 4$, $q = 3$ then

$$\begin{aligned}
\mu(G, N_G(H), g) &\leq \frac{q^8 \prod_{k=1}^{2} \left(1 - \frac{1}{q^{2k}}\right) \cdot \frac{212}{81} q^4}{q^{16} \prod_{k=1}^{4} \left(1 - \frac{1}{q^k}\right)} \\
&= \frac{3^8 \cdot 212}{3^{16} \cdot \frac{2}{3} \cdot \frac{26}{27}} \\
&= \frac{212}{52} \cdot \frac{1}{3^4} < \frac{1}{19} \, .
\end{aligned}$$

The proof of this lemma is now complete. ■

Lemma 4.3.14 *Let $G = Sp_d(q)$, q odd, $Sp_{\frac{d}{r}}(q^r) \simeq H < G$, r an odd prime divisor of d and $g \in N_G(H) \setminus H$ such that $g^r \in Z(G)$. Then*

$$\mu(G, N_G(H), g) < \frac{1}{q^{\frac{1}{2}d(r-1)}} \, .$$

Proof: As before, we will use Lemma 4.1.2 again, according to which

$$\mu(G, N_G(H), g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H), g)|}{|G|} \, .$$

Here,

$$|G| = q^{\frac{d^2}{2} + \frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right) ,$$

$$|\mathcal{C}(G, N_G(H), g)| < |N_G(H)| = r \cdot q^{\frac{d^2}{2r} + \frac{d}{2}} \prod_{k=1}^{\frac{d}{2r}} \left(1 - \frac{1}{q^{2rk}}\right)$$

and by Lemma 4.3.3/(c),

$$|C_G(g)| \leq q^{\frac{d^2+d}{2r}} \left(1 + \frac{1}{q}\right)^{r-1} .$$

Notice that

$$\frac{r \cdot \left(1+\frac{1}{q}\right)^{r-1}}{\prod_{k=1}^{\frac{d}{2}} \left(1-\frac{1}{q^{2k}}\right)} \leq q^r$$

since $\prod_{k=1}^{\frac{d}{2}} \left(1-\frac{1}{q^{2k}}\right) > \frac{q^2-2}{q^2-1} \geq \frac{7}{8}$, $r \cdot \frac{8}{7} < 3^{\frac{r}{2}} \leq q^{\frac{r}{2}}$ and $\left(1+\frac{1}{q}\right)^{r-1} < \left(\frac{4}{3}\right)^r < q^{\frac{r}{2}}$. Therefore

$$\mu(G, N_G(H), g) < q^{\frac{d^2}{r}-\frac{d^2}{2}+\frac{d}{2r}+r}$$

and the statement of the lemma is true whenever

$$\frac{d^2}{r} - \frac{d^2}{2} + \frac{d}{2r} + r \leq \frac{1}{2}d(r-1) ,$$

that is,

$$d^2(2-r) + d + 2r^2 \leq -dr(r-1) ,$$

$$dr(r-1) + d + 2r^2 \leq d^2(r-2) .$$

Since $d = nr$ for some positive even integer n, we can rewrite this inequality as

$$nr^2(r-1) + nr + 2r^2 \leq n^2r^2(r-2) ;$$

$$n(r-1) + \frac{n}{r} + 2 \leq n^2(r-2) ;$$

$$n\frac{r-1}{r-2} + \frac{n}{r(r-2)} + \frac{2}{r-2} \leq n^2 .$$

Now if $r \geq 5$ then

$$n\frac{r-1}{r-2} + \frac{n}{r(r-2)} + \frac{2}{r-2} \leq \frac{4n}{3} + \frac{n}{15} + \frac{2}{3} < 2n \leq n^2$$

for any $n \geq 2$, and if $r = 3$ then

$$n\frac{r-1}{r-2} + \frac{n}{r(r-2)} + \frac{2}{r-2} = 2n + \frac{n}{3} + 2 \leq n^2$$

whenever $n > 2$. This proves the lemma except for the case $d = 6$, $r = 3$. As we did in Lemma 4.3.12, we will handle this case by giving a stronger upper bound for $|\mathcal{C}(G, N_G(H), g)|$.

From now on, suppose that $d = 6$ and $r = 3$. Notice that in this case, q is not a power of 3. Since $g^3 = \alpha I$ with $\alpha = \pm 1$, clearly

$$\mathcal{C}(G, N_G(H), g) \subseteq \{h \in N_G(H) \setminus Z(G) \,|\, h^3 = \alpha I\} .$$

In general, if $A \in \mathrm{SL}_2(q_1)$ for some prime power q_1 then

$$A^3 = I \iff A = I \text{ or } \mathrm{Tr}(A) = -1$$

and

$$A^3 = -I \iff A = -I \text{ or } \mathrm{Tr}(A) = 1 .$$

The number of solutions for $a(\pm 1 - a) - bc = 1$ in $\mathbf{F}_{q_1}$ is

$$\begin{cases} q_1(q_1 - 1) & \text{if } x^2 \mp x + 1 \text{ does not factor in } \mathbf{F}_{q_1}[x] ; \\ q_1(q_1 + 1) & \text{if } x^2 \mp x + 1 \text{ factors in } \mathbf{F}_{q_1}[x] . \end{cases}$$

This fact together with Lemma 4.3.9 implies that

$$\begin{aligned} |\mathcal{C}(G, N_G(H), g)| &\leq 2\frac{|\mathrm{Sp}_2(q^2)|}{|\mathrm{Sp}_2(q)|} + q^6 + q^3 \\ &= 2\frac{q^3(q^6-1)}{q(q^2-1)} + q^6 + q^3 \\ &= 2q^2(q^4 + q^2 + 1) + q^6 + q^3 = 3q^6 + 2q^4 + q^3 + 2q^2 < 4q^6 , \end{aligned}$$

$$\begin{aligned} \mu(G, N_G(H), g) &< \frac{q^7\left(1 + \frac{1}{q}\right)^2 \cdot 4q^6}{q^{21} \prod_{k=1}^{3} \left(1 - \frac{1}{q^{2k}}\right)} \\ &< q^{-8} \cdot \frac{4 \cdot \left(1 + \frac{1}{q}\right)^2}{\frac{q^2-2}{q^2-1}} \\ &\leq q^{-8} \cdot 4 \cdot \left(\frac{6}{5}\right)^2 \cdot \frac{24}{23} \\ &< 7q^{-8} < q^{-6} = q^{\frac{1}{2}d(r-1)} . \end{aligned}$$

This completes the proof. ∎

Lemma 4.3.15 *Let $G = Sp_d(q)$, q odd, d divisible by 4, $Sp_{\frac{d}{2}}(q^2) \simeq H < G$ and $g \in N_G(H) \setminus H$ such that $g^2 = \pm I$.*

(a) *If $d \geq 8$ then $\mu(G, N_G(H), g) \leq \dfrac{1}{q^{\frac{d}{2}}}$.*

(b) *If $d = 4$ then $\mu(G, N_G(H), g) \leq \dfrac{q}{q^2 - 1}$.*

Proof: First we will find upper bounds for the cardinalities of the sets

$$\{h \in H \mid h^2 = I\} \text{ and } \{h \in H \mid h^2 = -I\}.$$

Assume that h is an element of $\mathrm{Sp}_{\frac{d}{2}}(q^2)$ with $h^2 = I$. Then the characteristic polynomial of h is $(x-1)^{n_1}(x+1)^{n_2}$ with some even integers n_1 and n_2 such that $n_1 + n_2 = \frac{d}{2}$ and by Theorem 3.5.19, the order of the centralizer of h in $\mathrm{Sp}_{\frac{d}{2}}(q^2)$ is

$$q^{n_1^2+n_1+n_2^2+n_2} \prod_{k=1}^{\frac{n_1}{2}} \Big(1 - \frac{1}{q^{4k}}\Big) \prod_{k=1}^{\frac{n_2}{2}} \Big(1 - \frac{1}{q^{4k}}\Big) > q^{n_1^2+n_2^2+\frac{d}{2}} \Big(\frac{q^4-2}{q^4-1}\Big)^2 .$$

Since the conjugacy class of h in $\mathrm{Sp}_{\frac{d}{2}}(q^2)$ is characterized by n_1 and n_2, we get from this that

$$\begin{aligned}
|\{h \in H \mid h^2 = I\}| &\leq \sum_{l=0}^{\frac{d}{4}} \frac{|\mathrm{Sp}_{\frac{d}{2}}(q^2)|}{q^{(2l)^2+(\frac{d}{2}-2l)^2+\frac{d}{2}}\big(\frac{q^4-2}{q^4-1}\big)^2} \\
&< \sum_{l=0}^{\frac{d}{4}} \frac{q^{\frac{d^2}{4}+\frac{d}{2}}}{q^{4l^2+\frac{d^2}{4}-2dl+4l^2+\frac{d}{2}}} \Big(\frac{q^4-1}{q^4-2}\Big)^2 \\
&= \sum_{l=0}^{\frac{d}{4}} q^{2l(d-4l)} \Big(\frac{q^4-1}{q^4-2}\Big)^2 \\
&\leq 2\sum_{k=0}^{\frac{d^2}{8}} q^k \Big(\frac{q^4-1}{q^4-2}\Big)^2 \\
&< \frac{2}{q-1}\Big(\frac{q^4-1}{q^4-2}\Big)^2 \cdot q^{\frac{d^2}{8}+1} .
\end{aligned}$$

Together with Lemma 4.3.9, this implies

$$\begin{aligned}
|\mathcal{C}(G, N_G(H), g)| &\leq \frac{|\mathrm{Sp}_{\frac{d}{2}}(q^2)|}{|\mathrm{Sp}_{\frac{d}{2}}(q)|} + \frac{2}{q-1}\Big(\frac{q^4-1}{q^4-2}\Big)^2 q^{\frac{d^2}{8}+1} \\
&= \frac{q^{\frac{d^2}{4}+\frac{d}{4}} \prod_{k=0}^{\frac{d}{4}} \big(1 - \frac{1}{q^{4k}}\big)}{q^{\frac{d^2}{8}+\frac{d}{2}} \prod_{k=0}^{\frac{d}{4}} \big(1 - \frac{1}{q^{2k}}\big)} + \frac{2}{q-1}\Big(\frac{q^4-1}{q^4-2}\Big)^2 q^{\frac{d^2}{8}+1} \\
&< q^{\frac{d^2}{8}+\frac{d}{4}} \cdot \frac{q^2-1}{q^2-2} + q^{\frac{d^2}{8}+1} \\
&< q^{\frac{d^2}{8}+\frac{d}{4}+1} .
\end{aligned}$$

If $d = 4$ then $H \simeq \mathrm{SL}_2(q^2)$, so

$$\{h \in H \mid h^2 = I\} = \{I, -I\}$$

and simply

$$\begin{aligned} |\mathcal{C}(G, N_G(H), g)| &= \frac{|\mathrm{Sp}_2(q^2)|}{|\mathrm{Sp}_2(q)|} \\ &= \frac{(q^2-1)q^2(q^2+1)}{(q-1)q(q+1)} = q(q^2+1)\ . \end{aligned}$$

Now assume that h is an element of $\mathrm{Sp}_{\frac{d}{2}}(q^2)$ with $h^2 = -I$. Then the characteristic polynomial of h is $(x-\mu)^{\frac{d}{4}}(x+\mu)^{\frac{d}{4}}$ where $\pm\mu$ are the square roots of -1 in the field $\mathbf{F}_{q^2}$. By Theorem 3.5.19, the order of the centralizer of h in $\mathrm{Sp}_{\frac{d}{2}}(q^2)$ is

$$q^{\frac{d^2}{8}} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right) .$$

Since in this case, $\{h \in H \mid h^2 = -I\}$ consists only of one conjugacy class of elements, we have

$$\begin{aligned} |\{h \in H \mid h^2 = I\}| &= \frac{|\mathrm{Sp}_{\frac{d}{2}}(q^2)|}{|C_g(h)|} \\ &= \frac{q^{\frac{d^2}{4}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{4k}}\right)}{q^{\frac{d^2}{8}} \prod_{k=1}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right)} \\ &< q^{\frac{d^2}{8}+\frac{d}{2}} \cdot \frac{q^2-1}{q^2-2} \end{aligned}$$

and then

$$\begin{aligned} |\mathcal{C}(G, N_G(H), g)| &< \frac{|\mathrm{Sp}_{\frac{d}{2}}(q^2)|}{|\mathrm{Sp}_{\frac{d}{2}}(q)|} + q^{\frac{d^2}{8}+\frac{d}{2}} \cdot \frac{q^2-1}{q^2-2} \\ &< q^{\frac{d^2}{8}+\frac{d}{4}} \frac{q^2-1}{q^2-2} + q^{\frac{d^2}{8}+\frac{d}{2}} \cdot \frac{q^2-1}{q^2-2} \\ &\leq q^{\frac{d^2}{8}+\frac{d}{2}} \cdot \frac{q^2-1}{q^2-2}\left(1 + \frac{1}{q}\right) \\ &\leq q^{\frac{d^2}{8}+\frac{d}{2}} \cdot \frac{8}{7} \cdot \frac{4}{3} = \frac{32}{21} \cdot q^{\frac{d^2}{8}+\frac{d}{2}}\ . \end{aligned}$$

If $d = 4$ then $H \simeq \mathrm{SL}_2(q^2)$ and

$$\{h \in H \mid h^2 = -I\} = \{h \in H \mid \mathrm{Tr}(h) = 0\} .$$

The number of solutions for $-a^2 - bc = 1$ in $\mathbf{F}_{q^2}$ is $q^2(q^2+1)$, so

$$|\{h \in H \mid h^2 = -I\}| = q^4 + q^2 ,$$

$$\begin{aligned} |\mathcal{C}(G, N_G(H), g)| &\leq \frac{|\mathrm{Sp}_2(q^2)|}{|\mathrm{Sp}_2(q)|} + q^2(q^2+1) \\ &= \frac{(q^2-1)q^2(q^2+1)}{(q-1)q(q+1)} + q^2(q^2+1) = q(q+1)(q^2+1) . \end{aligned}$$

So far we proved that

$$|\mathcal{C}(G, N_G(H), g)| \leq \begin{cases} q^{\frac{d^2}{8}+\frac{d}{4}+1} & \text{if } g^2 = I \text{ and } d \geq 8 ; \\ q(q^2+1) & \text{if } g^2 = I \text{ and } d = 4 ; \\ \frac{32}{21} \cdot q^{\frac{d^2}{8}+\frac{d}{2}} & \text{if } g^2 = -I \text{ and } d \geq 8 ; \\ q(q+1)(q^2+1) & \text{if } g^2 = -I \text{ and } d = 4 . \end{cases}$$

Now use the formula given by Lemma 4.1.2. If $g^2 = I$ then by Lemma 4.3.3, $|C_G(g)| = q^{\frac{d^2}{4}+\frac{d}{2}} \prod_{k=0}^{\frac{d}{4}} \left(1 - \frac{1}{q^{2k}}\right)$, so

$$\begin{aligned} \mu(G, N_G(H), g) &< \frac{q^{\frac{d^2}{4}+\frac{d}{2}} \cdot q^{\frac{d^2}{8}+\frac{d}{4}+1}}{q^{\frac{d^2}{2}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)} \\ &< \frac{q^{\frac{d^2}{4}+\frac{d}{2}} \cdot q^{\frac{d^2}{8}+\frac{d}{4}+1}}{q^{\frac{d^2}{2}+\frac{d}{2}-1}} \\ &= q^{\frac{d}{4}+2-\frac{d^2}{8}} \end{aligned}$$

and the statement of this lemma is true whenever

$$\frac{d}{4} + 2 - \frac{d^2}{8} \leq -\frac{d}{2} .$$

Since $d = 4k$ for some positive integer k, we can rewrite this inequality as

$$k + 2 - 2k^2 \leq 2k ;$$

$$3k + 2 \leq 2k^2$$

and this is true for any $k \geq 2$. If $d = 4$ then $|C_G(g)| = q^6(1 - \frac{1}{q^2})$, so

$$\begin{aligned} \mu(G, N_G(H), g) &\leq \frac{q^6(1-\frac{1}{q^2}) \cdot q(q^2+1)}{q^{10}(1-\frac{1}{q^2})(1-\frac{1}{q^4})} \\ &= \frac{q^6 q(q^2+1)}{q^6(q^4-1)} = \frac{q}{q^2-1}\,. \end{aligned}$$

If $g^2 = -I$ then by Lemma 4.3.3/(*b*), $|C_G(g)| \leq q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} (1 - \frac{(-1)^k}{q^k})$, so

$$\begin{aligned} \mu(G, N_G(H), g) &\leq \frac{q^{\frac{d^2}{4}}(1+\frac{1}{q}) \cdot \frac{32}{21} \cdot q^{\frac{d^2}{8}+\frac{d}{2}}}{q^{\frac{d^2}{2}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} (1-\frac{1}{q^{2k}})} \\ &< q^{-\frac{d^2}{8}} \cdot \left(1+\frac{1}{q}\right) \cdot \frac{32}{21} \cdot \frac{q^2-1}{q^2-2} \\ &\leq q^{-\frac{d^2}{8}} \cdot \frac{4}{3} \cdot \frac{32}{21} \cdot \frac{8}{7} = q^{-\frac{d^2}{8}} \cdot \frac{1024}{441} \\ &< q^{-\frac{d^2}{8}+1} \end{aligned}$$

and the theorem is true whenever $-\frac{d^2}{8} + 1 \leq -\frac{d}{2}$, that is $4d + 8 \leq d^2$. This is certainly true for $d \geq 8$. If $d = 4$, then $|C_G(g)| \leq q^4 \prod_{k=1}^{2} (1 - \frac{(-1)^k}{q^k})$, so

$$\begin{aligned} \mu(G, N_G(H), g) &\leq \frac{q^4(1+\frac{1}{q})(1-\frac{1}{q^2}) \cdot q(q+1)(q^2+1)}{q^{10}(1-\frac{1}{q^2})(1-\frac{1}{q^4})} \\ &= \frac{q(q+1)(q^2-1) \cdot q(q+1)(q^2+1)}{q^4(q^2-1)(q^4-1)} = \frac{q+1}{q^2(q-1)} \end{aligned}$$

and $\frac{q+1}{q^2(q-1)}$ is less then $\frac{q}{q^2-1}$ for any odd prime power q. ■

Lemma 4.3.16 *Let* $G = Sp_d(q)$*,* q *odd,* $d \equiv 2 \pmod 4$*,* $GU_{\frac{d}{2}}(q^2) \simeq H < G$ *and* $g \in N_G(H) \setminus H$ *such that* $g^2 = -I$*.*

(*a*) *If* $d = 2$ *and* $q \equiv 1 \pmod 4$ *then* $\mu(G, N_G(H), g) \leq \dfrac{1}{q}$.

(*b*) *If* $d = 2$ *and* $q \equiv 3 \pmod 4$ *then* $\mu(G, N_G(H), g) \leq \dfrac{q+3}{q(q-1)}$.

(*c*) *If* $d \geq 6$ *then* $\mu(G, N_G(H), g) \leq \dfrac{1}{q^{d-2}}$.

Proof: First we find an upper bound for the cardinality of the set $\{h \in H \mid h^2 = -I\}$. Assume h is an element in $\mathrm{GU}_{\frac{d}{2}}(q^2)$ with $h^2 = -I$. Then the characteristic polynomial of h is $(f_i(x))^{n_1}(f_j(x))^{n_2}$ where $f_i(x) = x - \mu$, $f_j(x) = x + \mu$, $\mu^2 = -1$ and $n_1 + n_2 = \frac{d}{2}$. From here, we have to separate two cases. If $q \equiv 1 \pmod 4$, then

$$x\bar{f}_i(x^{-1}) = x(x^{-1} - \bar{\mu}) = x(x^{-1} - \mu^q) = 1 - \mu x = -\mu(x + \mu) = -\mu f_j(x)$$

showing that $i' = j$ and hence $n_i = n_j$. But that is a contradiction, since $n_i + n_j = \frac{d}{2}$ and $\frac{d}{2}$ is an odd integer. If $q \equiv 1 \pmod 4$, then

$$x\bar{f}_i(x^{-1}) = x(x^{-1} - \bar{\mu}) = x(x^{-1} - \mu^q) = 1 + \mu x = \mu(x - \mu)$$

which means that $i = i'$ and $j = j'$. Then by Theorem 3.5.19, the order of the centralizer of h in $\mathrm{GU}_{\frac{d}{2}}(q^2)$ is

$$q^{n_1^2+n_2^2} \prod_{k=1}^{n_1} \left(1 - \frac{(-1)^k}{q^k}\right) \prod_{k=1}^{n_2} \left(1 - \frac{(-1)^k}{q^k}\right)$$

and the cardinality of the conjugacy class of h is

$$q^{\frac{d^2}{4} - n_1^2 - n_2^2} \frac{\prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{(-1)^k}{q^k}\right)}{\prod_{k=1}^{n_1} \left(1 - \frac{(-1)^k}{q^k}\right) \prod_{k=1}^{n_2} \left(1 - \frac{(-1)^k}{q^k}\right)} \leq q^{\frac{d^2}{4} - n_1^2 - n_2^2} .$$

Since n_1 and n_2 characterize the conjugacy class of h in $\mathrm{GL}_{\frac{d}{2}}(q^2)$, we have

$$\begin{aligned} |\{h \in H \mid h^2 = -I\}| &\leq \sum_{l=0}^{\frac{d}{2}} q^{\frac{d^2}{4} - l^2 - (\frac{d}{2} - l)^2} = \sum_{l=0}^{\frac{d}{2}} q^{l(d-2l)} \\ &= 2 \sum_{l=0}^{\frac{d}{4} - \frac{1}{2}} q^{l(d-2l)} \leq 2 \sum_{k=0}^{\frac{d^2}{8} - \frac{1}{2}} q^k \\ &< q^{\frac{d^2}{8} + \frac{1}{2}} . \end{aligned}$$

Now, by Lemma 4.3.10,

$$\begin{aligned} |\{h \in N_G(H) \setminus H \mid h^2 = -I\}| &= \frac{|\mathrm{GU}_{\frac{d}{2}}(q^2)|}{|\mathrm{O}_{\frac{d}{2}}(q)|} \\ &= \frac{q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{(-1)^k}{q^k}\right)}{2q^{\frac{d^2}{8} - \frac{d}{4}} \prod_{k=1}^{\frac{d}{4} - \frac{1}{2}} \left(1 - \frac{1}{q^{2k}}\right)} \\ &< \frac{1}{2} \cdot q^{\frac{d^2}{8} + \frac{d}{4}} \cdot \frac{q+1}{q} \cdot \frac{q^2 - 1}{q^2 - 2} \\ &< q^{\frac{d^2}{8} + \frac{d}{4}} \end{aligned}$$

and

$$|\mathcal{C}(G, N_G(H), g)| < q^{\frac{d^2}{8}+\frac{1}{2}} + q^{\frac{d^2}{8}+\frac{d}{4}} < q^{\frac{d^2}{8}+\frac{d}{4}+1} .$$

Then by Lemma 4.3.4,

$$|C_G(g)| \leq q^{\frac{d^2}{4}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{(-1)^k}{q^k}\right) < q^{\frac{d^2}{4}+\frac{1}{2}}$$

and by Lemma 4.1.2,

$$\begin{aligned} \mu(G, N_G(H), g) &= \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H), g)|}{|G|} \\ &< \frac{q^{\frac{d^2}{4}+\frac{1}{2}} \cdot q^{\frac{d^2}{8}+\frac{d}{4}+1}}{q^{\frac{d^2}{2}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \left(1 - \frac{1}{q^{2k}}\right)} \\ &< \frac{q^{\frac{d^2}{4}+\frac{1}{2}} \cdot q^{\frac{d^2}{8}+\frac{d}{4}+1}}{q^{\frac{d^2}{2}+\frac{d}{2}-\frac{1}{2}}} \\ &= q^{-\frac{d^2}{8}-\frac{d}{4}+2} . \end{aligned}$$

This implies that $\mu(G, N_G(H), g) < q^{-d+2}$ whenever $-\frac{d^2}{8} - \frac{d}{4} + 2 \leq -d + 2$, that is, $\frac{3d}{4} \leq \frac{d^2}{8}$ and this is true for $d \geq 6$.

Finally, if $d = 2$ then $H \simeq Z_{q+1}$ and thus

$$|\{h \in H \mid h^2 = -I\}| = \begin{cases} 2 & \text{if } q \equiv 3 \pmod 4 ; \\ 0 & \text{if } q \equiv 1 \pmod 4 , \end{cases}$$

$$|\mathcal{C}(G, N_G(H), g) \leq |\{h \in H \mid h^2 = -I\}| + |H| = |\{h \in H \mid h^2 = -I\}| + q + 1 .$$

In this case, by Lemma 4.3.4,

$$|C_G(g)| = \begin{cases} q\left(1 + \frac{1}{q}\right) = q + 1 & \text{if } q \equiv 3 \pmod 4 ; \\ q\left(1 - \frac{1}{q}\right) = q - 1 & \text{if } q \equiv 1 \pmod 4 , \end{cases}$$

while $|G| = |\mathrm{Sp}_2(q)| = (q-1)q(q+1)$, therefore

$$\mu(G, N_G(H), g) \leq \begin{cases} \frac{1}{q} & \text{if } q \equiv 1 \pmod 4 ; \\ \frac{q+3}{q(q-1)} & \text{if } q \equiv 3 \pmod 4 . \end{cases}$$

Now the proof of this lemma is complete. ■

Lemma 4.3.17 *Let* $G = GL_d(q)$, *d an odd prime number, q not divisible by d,* $GL_1(q^d) \simeq Z_{q^d-1} \simeq H < G$ *and* $g \in N_G(H) \setminus H$ *such that* $g^d \in Z(G)$.

$$\begin{array}{lll} (a) & \text{If } q = 2 \text{ then } \mu(G, N_G(H), g) \leq \dfrac{7(d-1)}{2^{(d-1)^2}} \,. \\ (b) & \text{If } q = 3 \text{ then } \mu(G, N_G(H), g) \leq \dfrac{3(d-1)}{3^{(d-1)^2}} \,. \\ (c) & \text{If } q \geq 4 \text{ then } \mu(G, N_G(H), g) \leq \dfrac{2(d-1)}{q^{(d-1)^2}} \,. \end{array}$$

Proof: Let $g^d = \alpha I$, $\alpha \in \mathbf{F}_q$. Since H is cyclic, $|\{h \in H \mid h^d = \alpha I\}| \leq d$ and then by Lemma 4.3.8,

$$|\mathcal{C}(G, N_G(H), g)| \leq (d-1)\frac{|\mathrm{GL}_1(q^d)|}{|\mathrm{GL}_1(q)|} + d = (d-1)\frac{q^d - 1}{q-1} + d \,.$$

Furthermore, by Lemma 4.3.2,

$$|C_G(g)| \leq q^d\Big(1 - \frac{1}{q^d}\Big) = q^d - 1 \,,$$

and then by Lemma 4.1.2,

$$\begin{aligned} \mu(G, N_G(H), g) &= \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H), g)|}{|G|} \\ &\leq \frac{(q^d-1)\cdot\big((d-1)\frac{q^d-1}{q-1} + d\big)}{q^{d^2}\prod_{k=1}^{d}\big(1 - \frac{1}{q^k}\big)} \\ &= \frac{(d-1)(q^d-1) + d(q-1)}{(q-1)q^{d^2-d}\prod_{k=1}^{d-1}\big(1 - \frac{1}{q^k}\big)} \\ &= \frac{(d-1)q^d + d(q-2) + 1}{(q-1)q^{d^2-d}\prod_{k=1}^{d-1}\big(1 - \frac{1}{q^k}\big)} \,. \end{aligned}$$

If $q = 2$ then

$$\frac{(d-1)q^d + d(q-2) + 1}{(q-1)q^{d^2-d}\prod_{k=1}^{d-1}\big(1 - \frac{1}{q^k}\big)} = \frac{(d-1)2^d + 1}{2^{d^2-d}\prod_{k=1}^{d-1}\big(1 - \frac{1}{2^k}\big)} =$$

$$= \frac{d-1}{2^{(d-1)^2}} \cdot \frac{1}{\prod_{k=1}^{d-1}\big(1 - \frac{1}{2^k}\big)} \cdot \Big[2 + \frac{1}{(d-1)2^{d-1}}\Big]$$

And we need to show that

$$\frac{1}{\prod_{k=1}^{d-1}\big(1 - \frac{1}{2^k}\big)} \cdot \Big[2 + \frac{1}{(d-1)2^{d-1}}\Big] \leq 7 \,.$$

If $d = 3$ then the left hand side of this inequality is

$$\frac{8}{3} \cdot \left[2 + \frac{1}{8}\right] = \frac{8}{3} \cdot \frac{17}{8} = \frac{17}{3} < 7 \, ,$$

if $d = 5$ then it is

$$\left(2 \cdot \frac{4}{3} \cdot \frac{8}{7} \cdot \frac{16}{15}\right) \cdot \left[2 + \frac{1}{64}\right] = \frac{1024}{315} \cdot \frac{129}{64} \approx 6.55 < 7 \, ,$$

and if $d \geq 7$ then

$$\prod_{k=1}^{d-1} \left(1 - \frac{1}{2^k}\right) \geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{8}\right)\left(1 - \sum_{k=0}^{\infty} \frac{1}{2^{k+4}}\right) = \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8} \cdot \frac{7}{8} = \frac{147}{512} \, ,$$

$$2 + \frac{1}{(d-1)2^{d-1}} \leq 2 + \frac{1}{6 \cdot 64} = \frac{769}{384}$$

and therefore

$$\frac{1}{\prod_{k=1}^{d-1} \left(1 - \frac{1}{2^k}\right)} \cdot \left[2 + \frac{1}{(d-1)2^{d-1}}\right] \leq \frac{512}{147} \cdot \frac{769}{384} = \frac{3076}{441} < \frac{3087}{441} = 7 \, .$$

This concludes the proof of (a).

If $q = 3$ then

$$\mu(G, N_G(H), g) \leq \frac{(d-1)q^d + d(q-2) + 1}{(q-1)q^{d^2-d} \prod_{k=1}^{d-1} \left(1 - \frac{1}{q^k}\right)} = \frac{(d-1)3^d + d + 1}{2 \cdot 3^{d^2-d} \prod_{k=1}^{d-1} \left(1 - \frac{1}{3^k}\right)} \, ,$$

$$\prod_{k=1}^{d-1} \left(1 - \frac{1}{3^k}\right) > \left(1 - \frac{1}{3}\right)\left(1 - \sum_{k=0}^{\infty} \frac{1}{3^{2+k}}\right) = \frac{2}{3} \cdot \frac{5}{6} = \frac{5}{9} \, ,$$

so

$$\mu(G, N_G(H)) < \frac{(d-1)3^d + d + 1}{2 \cdot 3^{d^2-d} \frac{5}{9}} = \frac{(d-1)3^d + d + 1}{10 \cdot 3^{d^2-d-2}} =$$

$$= \frac{d-1}{3^{(d-1)^2}} \cdot \frac{1}{10} \cdot \left[27 + \frac{d+1}{3^{d-3}(d-1)}\right]$$

and we need to show that,

$$\frac{1}{10} \cdot \left[27 + \frac{d+1}{3^{d-3}(d-1)}\right] \leq 3 ;$$

or equivalently,

$$27 + \frac{d+1}{3^{d-3}(d-1)} \leq 30 \, ,$$

$$\frac{d+1}{3^{d-3}(d-1)} \leq 3\,,$$
$$\frac{d+1}{d-1} \leq 3^{d-2}$$

and this is certainly true.

If $q \geq 4$ and $d = 3$ then

$$\frac{(d-1)q^d + d(q-2) + 1}{(q-1)q^{d^2-d}\prod_{k=1}^{d-1}\left(1 - \frac{1}{q^k}\right)} = \frac{2(q^3-1) + 3(q-1)}{(q-1)q^6(1-\frac{1}{q})(1-\frac{1}{q^2})}\,,$$
$$\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right) \geq \frac{3}{4} \cdot \frac{15}{16} = \frac{45}{64}\,,$$

so

$$\mu(G, N_G(H), g) \leq \frac{2(q^3-1) + 3(q-1)}{(q-1)q^6 \cdot \frac{45}{64}} = \frac{128(q^3-1)}{45(q-1)q^6} + \frac{64}{15 \cdot q^6} =$$
$$= \frac{1}{4} \cdot \left[\frac{128}{(q^3-1)}45(q-1)q^2 + \frac{64}{15q^2}\right]$$

and we need to show that

$$\frac{128}{(q^3-1)}45(q-1)q^2 + \frac{64}{15q^2} \leq 4\,,$$

that is,

$$\frac{32}{45}\left(1 + \frac{1}{q} + \frac{1}{q^2}\right) + \frac{16}{15 \cdot q^2} \leq 1$$

and equality holds here for $q = 4$, while the left hand side is a decreasing function of q.

Now suppose that $q = 4$ and $d \geq 5$. Then

$$\frac{(d-1)q^d + d(q-2) + 1}{(q-1) \cdot q^{d^2-d}\prod_{k=1}^{d-1}\left(1 - \frac{1}{q^k}\right)} = \frac{(d-1)4^d + 2d + 1}{3 \cdot 4^{d^2-d}\prod_{k=1}^{d-1}\left(1 - \frac{1}{4^k}\right)}\,,$$
$$\prod_{k=1}^{d-1}\left(1 - \frac{1}{q^k}\right) > \left(1 - \frac{1}{4}\right)\left(1 - \sum_{k=0}^{\infty}\frac{1}{4^{k+2}}\right) = \frac{3}{4} \cdot \frac{11}{12} = \frac{11}{16}\,,$$

so

$$\begin{aligned} \mu(G, N_G(H), g) &< \frac{(d-1)4^d + 2d + 1}{3 \cdot 4^{d^2-d}\prod_{k=1}^{d-1}\frac{11}{16}} \\ &= \frac{d-1}{4^{(d-1)^2}} \cdot \frac{11}{16} \cdot \left[\frac{4}{3} + \frac{2d+1}{3(d-1)4^{d^2-d}}\right]. \end{aligned}$$

We need to show that

$$\frac{11}{16}\cdot\left[\frac{4}{3}+\frac{2d+1}{3(d-1)4^{d^2-d}}\right]\leq 2\,,$$

that is

$$\begin{aligned}
\frac{4}{3}+\frac{2d+1}{3\cdot 4^{d^2-d}} &\leq \frac{11}{8}\,,\\
4+\frac{2d+1}{(d-1)4^{d^2-d}} &\leq \frac{33}{8}\,,\\
\frac{2d+1}{(d-1)4^{d^2-d}} &\leq \frac{1}{8}\,,\\
\frac{2d+1}{d-1} &\leq 2^{2d-5}
\end{aligned}$$

and this certainly true for $d \geq 5$.

Finally, assume that $q \geq 5$ and $d \geq 5$. Then

$$\begin{aligned}
\mu(G, N_G(H), g) &\leq \frac{(d-1)q^d + d(q-2)+1}{(q-1)\cdot q^{d^2-d}\prod_{k=1}^{d-1}\left(1-\frac{1}{q^k}\right)}\\
&< \frac{(d-1)q^d + d(q-2)+1}{(q-1)\cdot q^{d^2-d}\cdot\frac{q-2}{q-1}}\\
&= \frac{(d-1)q^d + d(q-2)+1}{(q-2)\cdot q^{d^2-d}}\\
&= \frac{d-1}{q^{(d-1)^2}}\cdot\left[\frac{q}{q-2}+\frac{d}{(d-1)q^{d-1}}+\frac{1}{(q-2)(d-1)q^{d-1}}\right]\\
&\leq \frac{d-1}{q^{(d-1)^2}}\cdot\left[\frac{5}{3}+\frac{5}{4\cdot 625}+\frac{1}{3\cdot 4\cdot 625}\right]\\
&= \frac{d-1}{q^{(d-1)^2}}\cdot\frac{12500+15+1}{7500} = \frac{d-1}{q^{(d-1)^2}}\cdot\frac{12516}{7500}\\
&< \frac{2(d-1)}{q^{(d-1)^2}}\,.
\end{aligned}$$

This completes the proof of this lemma. ∎

4.4 Case III: Elements of Order p Centralizing an Extension Field

In this section, as usual, d is a positive integer, r is a prime divisor of d, p a prime number, $q = p^f$ and V is a vector space of dimension d over $\mathbf{F}_q$ which is also a vector space of dimension $\frac{d}{r}$ over $\mathbf{F}_{q^r}$. As in Section 4.2, we will denote V by $\hat{V}$ when we consider it as a vector space over $\mathbf{F}_{q^r}$. Let $G = \mathrm{GL}_{\mathbf{F}_q}(V)$, $H = \mathrm{GL}_{\mathbf{F}_{q^r}}(\hat{V})$

and $g \in H \setminus Z(G)$ an element of order p that is not conjugate to any element of $N_G(H) \setminus H$.

Following the notations of Section 3.4, let $V_{a,1}$ denote the quotient module of the regular $\mathbf{F}_q\langle g\rangle$-module with dimension a over $\mathbf{F}_q$ and let $V_{a,b}$ be the direct sum of b copies of $V_{a,1}$. Similarly, let $\hat{V}_{a,1}$ denote the quotient module of the regular $\mathbf{F}_{q^r}\langle g\rangle$-module with dimension a over $\mathbf{F}_{q^r}$ and let $\hat{V}_{a,b}$ be the direct sum of b copies of $\hat{V}_{a,1}$. It is easy to see that in general,

$$\hat{V}_{a,b} \simeq V_{a,rb} \tag{4.12}$$

as $\mathbf{F}_q\langle g\rangle$-modules. Let

$$\hat{V} = \bigoplus_{i=1}^{e} \hat{V}_i\,, \quad \hat{V}_i \simeq \hat{V}_{a_i,b_i} \tag{4.13}$$

be the decomposition of $\hat{V}$ into a direct sum of homogeneous $\mathbf{F}_{q^r}\langle g\rangle$-modules where $1 \le a_i < a_j \le p$ for all $1 \le i < j \le e$. Then if V_i denotes $\hat{V}_i$ as an $\mathbf{F}_q\langle g\rangle$-module, then

$$V = \bigoplus_{i=1}^{e} V_i\,, \quad V_i \simeq V_{a_i,rb_i} \tag{4.14}$$

is a decomposition of V into a direct sum of homogeneous $\mathbf{F}_q\langle g\rangle$-modules. Notice that

$$\sum_{i=1}^{e} r a_i b_i = d\,. \tag{4.15}$$

Theorem 4.4.1 *Let $G = GL_d(q)$, $GL_{\frac{d}{r}}(q^r) \simeq H < G$ and $g \in H \setminus Z(G)$ an element of order p that is not conjugate to any element in $N_G(H) \setminus H$.*

(a) *If $r = \frac{d}{2}$ then $\mu(G, N_G(H), g) \le \frac{1}{q^{d(r-1)}} \cdot \frac{q^r}{q^r - 1}$.*

(b) *If $r \ne \frac{d}{2}$ then $\mu(G, N_G(H), g) \le \frac{1}{q^{d(r-1)}}$.*

Proof: By Theorem 3.4.11,

$$|C_G(g)| = q^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}(rb_i)(rb_j)} \prod_{i=1}^{e}\prod_{k=1}^{rb_i}\left(1-\frac{1}{q^k}\right),$$

$$|C_H(g)| = (q^r)^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e}\prod_{k=1}^{b_i}\left(1-\frac{1}{q^{rk}}\right).$$

Notice that the conjugacy class of g in G (which is characterized by the pairs (a_i, b_i) for $1 \le i \le e$) determines the conjugacy class of g in H, that is, $g^G \cap H = g^H$. Then by Lemma 4.1.3,

$$N(G, N_G(H), g) = N(G, H, g) = \frac{1}{r} \cdot \frac{|C_G(g)|}{|C_H(g)|}$$

and by Lemma 4.1.1,

$$\mu(G, N_G(H), g) = \frac{N(G, N_G(H), g)}{|G : N_G(H)|} = \frac{1}{r} \cdot \frac{|N_G(H)|}{|G|} \cdot \frac{|C_G(g)|}{|C_H(g)|} = \frac{|H|}{|G|} \cdot \frac{|C_G(g)|}{|C_H(g)|} =$$

$$= \frac{q^{\frac{d^2}{r}} \prod_{k=1}^{\frac{d}{r}}\left(1-\frac{1}{q^{rk}}\right)}{q^{d^2}\prod_{k=1}^{d}\left(1-\frac{1}{q^d}\right)} \cdot \frac{q^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}(rb_i)(rb_j)} \prod_{i=1}^{e}\prod_{k=1}^{rb_i}\left(1-\frac{1}{q^k}\right)}{q^{r\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e}\prod_{k=1}^{b_i}\left(1-\frac{1}{q^{rk}}\right)}$$

that is,

$$\mu(G, N_G(H), g) = q^{\frac{1-r}{r}d^2 + r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \cdot \frac{\prod\limits_{i=1}^{e}\prod\limits_{\substack{1\le k\le rb_i\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)}{\prod\limits_{\substack{1\le k\le d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)}. \tag{4.16}$$

Notice that

$$\frac{\prod\limits_{i=1}^{e}\prod\limits_{\substack{1\le k\le rb_i\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)}{\prod\limits_{\substack{1\le k\le d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)} \le \frac{1}{\prod\limits_{\substack{r+1\le k\le d\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)} < \frac{1}{\prod\limits_{k=r+1}^{\infty}\left(1-\frac{1}{q^k}\right)}$$

and

$$\prod_{k=r+1}^{\infty}\left(1-\frac{1}{q^k}\right) > 1 - \sum_{k=r+1}^{\infty}\frac{1}{q^k} = 1 - \frac{1}{q^{r+1}-q^r} \le 1 - \frac{1}{q^r} = \frac{q^r-1}{q^r},$$

and hence from (4.16) we get

$$\mu(G, N_G(H), g) < q^{\frac{1-r}{r}d^2 + r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \cdot \frac{q^r}{q^r-1}. \tag{4.17}$$

Since $\frac{q^r}{q^r-1} < q$, $\mu(G, N_G(H), g) < q^{-d(r-1)}$ whenever

$$\frac{1-r}{r}d^2 + r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i, a_j\}b_i b_j + 1 \leq -d(r-1) ,$$

that is,

$$d(r-1) + r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i, a_j\}b_i b_j < \frac{r-1}{r}d^2 . \tag{4.18}$$

We will show that this is always true, unless $e = 1$, $a_1 = 2$ and $b_1 = 1$. Since

$$\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i, a_j\}b_i b_j \leq \sum_{i=1}^{e}\sum_{j=1}^{e}a_i b_i b_j = \Big(\sum_{i=1}^{e}a_i b_i\Big)\cdot\Big(\sum_{j=1}^{e}b_j\Big) = \frac{d}{r}\Big(\sum_{j=1}^{e}b_j\Big) ,$$

equation (4.18) follows from

$$d(r-1) + d(r-1)\sum_{j=1}^{e}b_j < \frac{r-1}{r}d^2 ,$$

which is equivalent to

$$1 + \sum_{j=1}^{e}b_j < \frac{d}{r} = \sum_{j=1}^{e}a_j b_j .$$

If $a_e \geq 3$ or $a_e = 2$ and $b_e \geq 2$ then $a_e b_e \geq 2 + b_e$ and so $2 + \sum_{j=1}^{e} b_j \leq \sum_{j=1}^{e} a_j b_j$. This proves the theorem unless $a_e = 2$ and $b_e = 1$. (Notice that a_e has to be at least 2 because $a_e = 1$ would mean $g = I$.)

Now assume that $\hat{V} = \hat{V}_1 \oplus \hat{V}_2$, $a_1 = 1$, $b_1 \geq 0$, $a_2 = 2$ and $b_2 = 1$. Then $d = ra_1b_1 = 2r$ and

$$\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i, a_j\}b_i b_j = a_1 b_1^2 + 2a_1 b_1 b_2 + a_2 b_2^2 = b_1^2 + 2b_1 + 2 ,$$

hence (4.18) holds whenever

$$d(r-1) + r(r-1)(b_1^2 + 2b_1 + 2) < \frac{r-1}{r}d^2 ,$$

$$d + r(b_1^2 + 2b_1 + 2) < \frac{1}{r}d^2 ,$$

$$\Big(r\sum_{i=1}^{e}a_i b_i\Big) + r(b_1^2 + 2b_1 + 2) < \frac{1}{r}\Big(r\sum_{i=1}^{e}a_i b_i\Big)^2 ,$$

$$r(b_1+2)+r(b_1^2+2b_1+2)<r(b_1+2)^2\ ,$$

$$b_1^2+3b_1+4<(b_1+2)^2\ ,$$

and this is true whenever b_1 is positive.

Finally, if $\hat{V}\simeq\hat{V}_{2,1}$ then $\frac{d}{r}=2$ and by (4.16),

$$\begin{aligned}\mu(G,N_G(H),g) &= q^{\frac{1-r}{r}(2r)^2+r(r-1)2}\cdot\frac{\prod\limits_{k=1}^{r-1}\left(1-\frac{1}{q^k}\right)}{\prod\limits_{\substack{1\leq k\leq 2r\\ r\nmid k}}\left(1-\frac{1}{q^k}\right)}\\ &= q^{-2r(r-1)}\cdot\frac{1}{\prod_{k=r+1}^{2r-1}\left(1-\frac{1}{q^k}\right)}\end{aligned}$$

and

$$\prod_{k=r+1}^{2r-1}\left(1-\frac{1}{q^k}\right)>1-\sum_{k=r+1}^{\infty}\frac{1}{q^k}=1-\frac{1}{q^{r+1}-q^r}\geq 1-\frac{1}{q^r}=\frac{q^r-1}{q^r}\ .$$

This proves (b). ∎

- - - - - - - - - - - - - - - - - - - -

Next, assume that q is odd, $\frac{d}{r}$ is even, let B be a non-singular symplectic form on V, $G_1=I(V,B)$ be the isometry group of (V,B) and $H_1=H\cap I(V,B)$. Furthermore, assume that H_1 contains a Singer cycle of $I(V,B)$ (that is, $H_1\simeq \mathrm{Sp}_{\frac{d}{r}}(q^r)$) and $g\in H_1$ an element of order p that is not conjugate to any element of $N_{G_1}(H_1)\setminus H_1$ in G_1. In other words, $\mathcal{C}(G_1,N_{G_1}(H_1),g)=\mathcal{C}(G_1,H_1,g)$. From Lemma 2.2.9 we know that H_1 is the isometry group of some $\mathbf{F}_{q^r}$-linear symplectic form on $\hat{V}$. Namely, $H_1=I(\hat{V},B_1)$ where

$$\begin{aligned}B_1:\hat{V}\times\hat{V} &\longrightarrow Z(H)\cup\{0\}\\ (u,v) &\longmapsto \sum_{\lambda\in Z(H)}B(u\lambda^{-1},v)\lambda\ .\end{aligned}$$

Recall from the proof of Lemma 2.2.9 that we also have

$$B(u,v)=-\mathrm{Tr}(B_1(u,v)) \tag{4.19}$$

for all $u, v \in V$ where Tr is the trace map from $Z(H) \cup \{0\} \simeq \mathbf{F}_{q^r}$ to $Z(G) \cup 0 \simeq \mathbf{F}_q$. We may assume that the decomposition of $\hat{V}$ in (4.13) is an orthogonal decomposition and then because of (4.19), the B_1-orthogonality of the decomposition $\hat{V} = \bigoplus_{i=1}^{e} \hat{V}_i$ implies the B-orthogonality of the decomposition $V = \bigoplus_{i=1}^{e} V_i$.

Lemma 4.4.2

$$\frac{|C_{G_1}(g)|}{|C_{H_1}(g)|} < q^{\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{1}{2}} .$$

Proof: By Theorem 3.4.13,

$$\begin{aligned} C_{G_1}(g) &= q^{\frac{1}{2}\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}(rb_i)(rb_j)}\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{rb_i}{2}\rfloor}(1-\frac{1}{q^{2k}})\cdot\rho(V_i,B,g) , \\ C_{H_1}(g) &= (q^r)^{\frac{1}{2}\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j}\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{b_i}{2}\rfloor}(1-\frac{1}{q^{2rk}})\cdot\rho(\hat{V}_i,B_1,g) , \end{aligned}$$

where

$$\rho(V_i,B,g) = \begin{cases} 2 & \text{if } a_i \text{ is even and } rb_i \text{ is odd ;} \\ \frac{2q^{\frac{rb_i}{2}}}{q^{\frac{rb_i}{2}}\pm1} & \text{if } a_i \text{ and } rb_i \text{ are both even ;} \\ q^{\frac{rb_i}{2}} & \text{if } a_i \text{ is odd ;} \end{cases}$$

$$\rho(\hat{V}_i,B_1,g) = \begin{cases} 2 & \text{if } a_i \text{ is even and } b_i \text{ is odd ;} \\ \frac{2q^{\frac{rb_i}{2}}}{q^{\frac{rb_i}{2}}\pm1} & \text{if } a_i \text{ and } b_i \text{ are both even ;} \\ q^{\frac{rb_i}{2}} & \text{if } a_i \text{ is odd .} \end{cases}$$

The statement of this lemma follows if we can show that

$$\frac{\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{rb_i}{2}\rfloor}(1-\frac{1}{q^{2k}})}{\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{b_i}{2}\rfloor}(1-\frac{1}{q^{2rk}})}\cdot\prod_{i=1}^{e}\frac{\rho(V_i,B,g)}{\rho(\hat{V}_i,B_1,g)} < q^{\frac{1}{2}} .$$

Since obviously

$$\frac{\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{rb_i}{2}\rfloor}(1-\frac{1}{q^{2k}})}{\prod_{i=1}^{e}\prod_{k=1}^{\lfloor\frac{b_i}{2}\rfloor}(1-\frac{1}{q^{2rk}})} \leq 1$$

It is enough to show that

$$\prod_{i=1}^{e}\frac{\rho(V_i,B,g)}{\rho(\hat{V}_i,B_1,g)} < q^{\frac{1}{2}} .$$

From the formula given above,

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, B_1, g)} = 1$$

whenever a_i is odd or a_i is even and rb_i is odd. Furthermore,

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, B_1, g)} \leq \frac{q^{\frac{rb_i}{2}} + 1}{q^{\frac{rb_i}{2}} - 1} \leq \frac{q^2 + 1}{q^2 - 1} < \frac{q(q+1)}{q^2 - 1} = \frac{q}{q-1}$$

if both a_i and b_i are even. Finally, if a_i is even, b_i is odd and $r = 2$ then

$$\frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, B_1, g)} \leq \frac{q^{\frac{rb_i}{2}}}{q^{\frac{rb_i}{2}-1}} = \frac{q^{b_i}}{q^{b_i} - 1} \leq \frac{q}{q-1} .$$

Hence

$$\begin{aligned} \prod_{i=1}^{e} \frac{\rho(V_i, B, g)}{\rho(\hat{V}_i, B_1, g)} &\leq \prod_{i, a_i \text{ even}} \frac{q}{q-1} \\ &\leq \left(\frac{p}{p-1}\right)^{\frac{p-1}{2}} \\ &< \sqrt{\exp(1)} < \sqrt{q} . \end{aligned}$$

This completes the proof. ∎

Lemma 4.4.3 *The number of conjugacy classes of H_1 that fall into the conjugacy class of g in G_1 is at most $2\sqrt{\frac{q}{r}}$.*

Proof: Because of Theorem 3.2.17, for each $1 \leq i \leq e$, the number of conjugacy classes of $I(\hat{V}_i, B_1)$ that fall into the conjugacy class of $g \mid_{\hat{V}_i}$ in $\mathrm{GL}(\hat{V}_i)$ is 2 if a_i is even and 1 if a_i is odd. Furthermore, the conjugacy class of $g \mid_{\hat{V}_i}$ in $\mathrm{GL}(\hat{V}_i)$ is the intersection if the conjugacy class of $g \mid_{\hat{V}_i}$ in $\mathrm{GL}(V_i)$ with $\mathrm{GL}(\hat{V}_i)$. Therefore, the number of conjugacy classes of $I(\hat{V}_i, B_1)$ that fall into the conjugacy class of $g \mid_{\hat{V}_i}$ in $I(V_i, B)$ is 1 if a_i is odd and is at most 2 if a_i is even.

Since the conjugacy class of g in $I(\hat{V}, B_1)$ /and in $I(V, B)$/ is characterized by the conjugacy classes of the restrictions of g to the subspaces V_i $(1 \leq i \leq e)$, in

$I(\hat{V}_i, B_1)$ /and $I(V_i, B)$, respectively/, it follows that the number of conjugacy classes of H_1 that fall into the conjugacy class of g in G_1 is at most 2^k where

$$k = |\{i \mid a_i \text{ even }\}| \,.$$

Of course, then $\sum_{i=1}^{e} a_i$ is greater than or equal to the sum of the first k even numbers, that is,

$$k(k+1) \leq \sum_{i=1}^{e} a_i \leq \sum_{i=1}^{e} a_i b_i = \frac{d}{r} \,,$$

and this implies $k < \sqrt{\frac{d}{r}}$. ■

Theorem 4.4.4 *Let $G_1 = Sp_d(q)$, q odd, $\frac{d}{r}$ even, $Sp_{\frac{d}{r}}(q^r) \simeq H_1 < G_1$ and $g \in H_1 \backslash Z(G_1)$ an element of order p that is not conjugate to any element of $N_{G_1}(H_1) \backslash H_1$.*

$$(a) \qquad \text{If } \frac{d}{r} = 2 \text{ then } \mu(G_1, N_{G_1}(H_1), g) \leq \frac{2}{q^{r(r-1)}} \cdot \frac{q^r}{q^r - 1} \,.$$

$$(b) \qquad \text{If } \frac{d}{r} \neq 2 \text{ then } \mu(G_1, N_{G_1}(H_1), g) \leq \frac{1}{q^{\frac{1}{2}d(r-1)}} \,.$$

By the previous two lemmas, if $g_1, g_2 \ldots, g_k$ are representatives of the conjugacy classes of H which are conjugate to g in G, then

$$\sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(g_i)|} < 2\sqrt{\tfrac{d}{r}} \cdot q^{\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{1}{2}} \,.$$

Then by Lemma 4.1.3/(b),

$$\begin{aligned}
\mu(G_1, N_{G_1}(H_1), g) &< \frac{|H_1|}{|G_1|} \cdot q^{\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{1}{2}} \cdot 2\sqrt{\tfrac{d}{r}} \\
&= \frac{q^{\frac{d^2}{2r}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2r}} \left(1 - \frac{1}{q^{2rk}}\right)}{q^{\frac{d^2}{2}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{r}} \left(1 - \frac{1}{q^{2k}}\right)} \cdot q^{\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{1}{2}} \cdot 2\sqrt{\tfrac{d}{2}} \\
&< q^{-\frac{r-1}{2r}d^2} \cdot \frac{q^2-1}{q^2-2} \cdot q^{\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{1}{2}+\sqrt{\frac{d}{r}}} \\
&< q^{-\frac{r-1}{2r}d^2+\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+1+\sqrt{\frac{d}{r}}}
\end{aligned}$$

This implies that $\mu(G_1, N_{G_1}(H_1), g) \leq \frac{1}{q^{\frac{1}{2}d(r-1)}}$ whenever

$$-\frac{r-1}{2r}d^2 + \frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j + 1 + \sqrt{\frac{d}{r}} \leq -\frac{1}{2}d(r-1) \,,$$

that is,

$$\frac{1}{2}d(r-1)+\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+1+\sqrt{\frac{d}{r}}\le\frac{r-1}{2r}d^2\,,$$

$$d+r\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+\frac{2}{r-1}+\sqrt{\frac{4d}{r(r-1)^2}}\le\frac{1}{r}d^2\,. \tag{4.20}$$

Since

$$r\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j\le r\sum_{i=1}^{e}\sum_{j=1}^{e}a_ib_ib_j=\Big(\sum_{i=1}^{e}ra_ib_i\Big)\Big(\sum_{j=1}^{e}b_j\Big)=d\sum_{j=1}^{e}b_j$$

equation (4.20) is true whenever

$$d+d\sum_{j=1}^{e}b_j+\frac{2}{r-1}+\sqrt{\frac{4d}{r(r-1)^2}}\le\frac{1}{r}d^2\,,$$

that is,

$$1+\frac{2}{d(r-1)}+\sqrt{\frac{4}{rd(r-1)^2}}+\sum_{j=1}^{e}b_j\le\frac{d}{r}=\sum_{j=1}^{e}a_jb_j\,. \tag{4.21}$$

As we mentioned in the proof of Theorem 4.4.1, $\sum_{j=1}^{e}b_j+2\le\sum_{j=1}^{e}a_jb_j$ if $a_e\ge 3$ or $a_e=2$ and $b_e\ge 2$. In these cases we also have

$$1+\frac{2}{d(r-1)}+\sqrt{\frac{4}{rd(r-1)^2}}\le 2$$

since $a_e\ge 3$ implies $d\ge 2a_3=6$, $\frac{2}{d}\le\frac{1}{3}$, $\sqrt{\frac{4}{rd}}\le\frac{1}{\sqrt{3}}$, and a_e2, $b_e\ge 2$ implies $d\ge 2a_eb_e=8$, $\frac{2}{d}\le\frac{1}{4}$ and $\sqrt{\frac{4}{rd}}\le\frac{1}{2}$. Hence equation (4.21) holds whenever $a_e\ge 3$ or $a_e=2$ and $b_e\ge 2$.

Now suppose $e=2$, $a_1=1$, $b_1\ge 0$, $a_2=2$ and $b_2=1$. Then $d=r(2+b_1)$ and in this case the number of conjugacy classes of H_1 that fall into the conjugacy class of g in G_1 is at most two. Therefore,

$$\begin{aligned}\mu(G_1,N_{G_1}(H_1),g) &< q^{-\frac{r-1}{2r}d^2+\frac{1}{2}r(r-1)\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j+1}\cdot 2\\ &< q^{-\frac{1}{2}r(r-1)(2+b_1)^2+\frac{1}{2}r(r-1)(b_1^2+2b_1+2)+2}\end{aligned}$$

and $\mu(G_1, N_{G_1}(H_1), g) < q^{-\frac{1}{2}d(r-1)} = q^{-\frac{1}{2}r(r-1)(2+b_1)}$ whenever

$$-\frac{1}{2}r(r-1)(2+b_1)^2 + \frac{1}{2}r(r-1)(b_1^2+2b_1+2) + 2 \leq -\frac{1}{2}r(r-1)(2+b_1)\,,$$

that is,

$$\begin{aligned} (2+b_1) + (b_1^2+2b_1+2) + \frac{4}{r(r-1)} &\leq (2+b_1)^2\,, \\ \frac{4}{r(r-1)} &\leq b_1\,. \end{aligned}$$

This is always true if b_1 is positive. (Notice that since $\frac{d}{r} = 2 + b_1$ is even, b_1 has to be an even integer.)

Finally, consider the case when $e = 1$, $a_1 = 2$ and $b_1 = 1$. Then $\frac{d}{r} = a_1 b_1 = 2$ and From Theorem 3.2.16,

$$\begin{aligned} \frac{|C_{G_1}(g)|}{|C_{H_1}(g)|} &= \frac{q^{\frac{1}{2}a_1(rb_1)^2}\prod_{k=1}^{\lfloor\frac{rb_1}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right)\cdot\rho(V,B,g)}{(q^r)^{\frac{1}{2}a_1b_1^2}\prod_{k=1}^{\lfloor\frac{b_1}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right)\cdot\rho(\hat{V},B_1,g)} \\ &= \frac{q^{r^2}\prod_{k=1}^{\lfloor\frac{r}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right)\cdot\rho(V,B,g)}{q^r\cdot 2} \\ &= q^{r(r-1)}\prod_{k=1}^{\lfloor\frac{r}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right)\cdot\frac{\rho(V,B,g)}{2} \\ &= \begin{cases} q^{r(r-1)}\prod_{k=1}^{\lfloor\frac{r}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right) & \text{if } r \text{ is odd}\ ; \\ q^2 & \text{if } r=2\ . \end{cases} \end{aligned}$$

Furthermore,

$$\frac{|H_1|}{|G_1|} = \frac{q^{2r+r}\left(1-\frac{1}{q^{2r}}\right)}{q^{2r^2+r}\prod_{k=1}^{r}\left(1-\frac{1}{q^{2k}}\right)} = q^{-2r(r-1)}\cdot\frac{1}{\prod_{k=1}^{r-1}\left(1-\frac{1}{q^{2k}}\right)}$$

and Therefore, by Lemma 4.1.3/(*b*),

$$\begin{aligned} \mu(G_1, N_{G_1}(H_1), g) &\leq 2\cdot q^{r(r-1)}\prod_{k=1}^{\lfloor\frac{r}{2}\rfloor}\left(1-\frac{1}{q^{2k}}\right)\cdot q^{-2r(r-1)}\cdot\frac{1}{\prod_{k=1}^{r-1}\left(1-\frac{1}{q^{2k}}\right)} \\ &= 2\cdot q^{-r(r-1)}\frac{1}{\prod_{k=\lfloor\frac{r}{2}\rfloor+1}^{r-1}\left(1-\frac{1}{q^{2k}}\right)} \\ &< 2\cdot q^{-r(r-1)}\frac{1}{\prod_{k=r+1}^{\infty}\left(1-\frac{1}{q^{k}}\right)} \\ &< 2\cdot q^{-r(r-1)}\frac{q^r}{q^r-1}\,, \end{aligned}$$

if r is odd, and

$$\begin{aligned}\mu(G_1, N_{G_1}(H_1), g) &\leq 2 \cdot q^2 \cdot q^{-4} \cdot \frac{1}{(1 - \frac{1}{q^2})} \\ &= \frac{2}{q^2 - 1} ,\end{aligned}$$

if $r = 2$.

Theorem 4.4.5 *Let* $G_1 = Sp_d(q)$*,* q *and* $\frac{d}{2}$ *odd,* $GU_{\frac{d}{2}}(q^2) \simeq H_1 < G_1$ *and* $g \in H_1 \backslash Z(G_1)$ *an element of order* p *that is not conjugate to any element of* $N_{G_1}(H_1) \backslash H_1$*. Then*

$$\mu(G_1, N_{G_1}(H_1)) \leq \frac{1}{q^{d-2}} .$$

By Theorem 3.4.12,

$$\begin{aligned}|C_{H_1}(g)| &= q^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e}\prod_{k=1}^{b_i}\Big(1 - \frac{(-1)^k}{q^k}\Big) \\ &> q^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} ,\end{aligned}$$

by Theorem 3.4.13,

$$\begin{aligned}|C_{G_1}(g)| &= q^{\frac{1}{2}\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}(2b_i)(2b_j)} \prod_{i=1}^{e}\prod_{k=1}^{b_i}\Big(1 - \frac{1}{q^{2k}}\Big)\rho(V_i, B, g) \\ &< q^{\frac{1}{2}\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}(2b_i)(2b_j)} \prod_{i=1}^{e}\rho(V_i, B, g) ,\end{aligned}$$

where

$$\rho(V_i, B, g) = \begin{cases} \frac{2q^b}{q^b \pm 1} & \text{if } a \text{ is even ;} \\ q^b & \text{if } a \text{ is odd .} \end{cases}$$

Also,

$$\begin{aligned}\frac{|H_1|}{|G_1|} &= \frac{q^{\frac{d^2}{4}}\prod_{k=1}^{\frac{d}{2}}(1 - \frac{(-1)^k}{q^k})}{q^{\frac{d^2}{2}+\frac{d}{2}}\prod_{k=1}^{\frac{d}{2}}(1 - \frac{1}{q^{2k}})} \\ &= q^{-\frac{d^2}{4}-\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \frac{1}{(1 + \frac{(-1)^k}{q^k})} \\ &= q^{-\frac{d^2}{4}-\frac{d}{2}} \prod_{k=1}^{\frac{d}{2}} \frac{q^k}{q^k + (-1)^k} \\ &< q^{-\frac{d^2}{4}-\frac{d}{2}} \frac{q}{q-1} < q^{-\frac{d^2}{4}-\frac{d}{2}+\frac{1}{2}} .\end{aligned}$$

And because of Theorem 3.3.8, the conjugacy class of g in G_1 (even more, the conjugacy class of g in $\mathrm{GL}(V)$) intersects H_1 in a single conjugacy class of H_1. Now, by using the formula given in Lemma 4.1.3/(*b*),

$$\begin{aligned} \mu(G_1, N_{G_1}(H_1), g) &= \frac{|H_1|}{|G_1|} \cdot \frac{|C_{G_1}(g)|}{|C_{H_1}(g)|} \\ &< q^{-\frac{d^2}{4}-\frac{d}{2}+\frac{1}{2}} \cdot q^{\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e} \rho(V_i, B, g) \\ &= q^{-\frac{d^2}{4}-\frac{d}{2}+\frac{1}{2}+\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e} \rho(V_i, B, g) \end{aligned}$$

and the statement of this theorem holds whenever

$$q^{\frac{d}{2}-\frac{3}{2}+\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j} \prod_{i=1}^{e} \rho(V_i, B, g) < q^{\frac{d^2}{4}} . \tag{4.22}$$

Since

$$\prod_{i=1}^{e} \rho(V_i, B, g) \le \prod_{i=1}^{e} q^{b_i}$$

and

$$\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j \le \sum_{i=1}^{e}\sum_{j=1}^{e} a_ib_ib_j = \frac{d}{2}\sum_{j=1}^{e} b_j ,$$

(4.22) is true whenever

$$\begin{aligned} \frac{d}{2} - \frac{3}{2} + (\frac{d}{2}+1)\sum_{j=1}^{e} b_j &\le \frac{d^2}{4} , \\ 2d - 6 + 2(d+2)\sum_{j=1}^{e} b_j \le d^2 . \end{aligned}$$

As we already mentioned it before, $\sum_{j=1}^{e} b_j \le \sum_{j=1}^{e} a_jb_j - 2 = \frac{d}{2} - 2$ if either $a_e \ge 3$ or $a_e = 2$ and $b_e \ge 2$. In that case,

$$\begin{aligned} 2d - 6 + 2(d+2)\sum_{j=1}^{e} b_j &\le 2d - 6 + 2(d+2)(\frac{d}{2} - 2) = 2d - 6 + (d+2)(d-4) \\ &= 2d - 6 + (d^2 - 2d - 8) < d^2 . \end{aligned}$$

Now suppose that $a_1 = 1$, $b_1 > 0$, $a_2 = 2$ and $b_2 = 1$. Then $d = 2(b_1 + 2)$, $\sum_{i=1}^{e}\sum_{j=1}^{e}\min\{a_i,a_j\}b_ib_j = b_1^2 + 2b_1 + 2$ and $\sum_{j=1}^{e} b_j = b_1 + 1$, therefore (4.22) holds whenever

$$\begin{aligned} q^{(b_1+2)-\frac{3}{2}+(b_1^2+2b_1+2)+(b_1+1)} &\leq q^{(b_1+2)^2} \\ (b_1+2)-\frac{3}{2}+(b_1^2+2b_1+2)+(b_1+1) &\leq (b_1+2)^2 \\ b_1^2+4b_1+\frac{7}{2} &\leq b_1^2+4b_1+4 , \end{aligned}$$

and this is true for any integer b_1.

4.5 Case IV: Elements of Order p Acting Non-Trivially on an Extension Field

Throughout this section, d is a positive integer, p is a prime divisor of d and q is a power of p. Furthermore, we will use the notation $V_{a,b}$ as in the previous section, for the direct sum of b copies of the a-dimensional quotient of the regular $\mathbf{F}_q Z_p$-module.

Lemma 4.5.1 *Let V be a vector space of dimension d over $\mathbf{F}_q$, $G = GL(V)$, H a subgroup of G such that $GL_{\frac{d}{p}}(q^p)$ and $g \in N_G(H) \setminus H$ with $g^p = I$. Then*

$$V \simeq V_{p,\frac{d}{p}}$$

as $\mathbf{F}_q\langle g\rangle$-modules.

Proof: Let $F = Z(H) \cup \{0\}$, so $F \simeq \mathbf{F}_{q^p}$, and let $\beta = \{v_1, v_2, \ldots , v_{\frac{d}{p}}\}$ be a basis of V over F. Let x be a normal element of the extension $F|\mathbf{F}_q$, that is, $\{x, x^q, \ldots , x^{q^{p-1}}\}$ is a basis of F over $\mathbf{F}_q$. Then the set

$$\{v_i x^{q^j} \mid 1 \leq i \leq \frac{d}{p} , 0 \leq j \leq p-1\}$$

is a basis of V over $\mathbf{F}_q$ and if we define

$$\begin{aligned} \sigma : V &\longrightarrow V \\ v_i x^{q^j} &\longmapsto v_i x^{q^{j+1}} , \end{aligned}$$

then $N_G(H) = \langle\sigma\rangle \ltimes H$. Notice that we also have $(v_i\alpha)\sigma = v_i\alpha^q$ for all i and $\alpha \in \mathbf{F}_{q^p}$.

Let R be the set of $\mathbf{F}_{q^p}$-linear transformations of V that correspond to the lower unitriangular matrices with respect to the basis β. That is, $h \in H$ belong to R if and only if $v_i h - v_i \in \langle v_j \,|\, j \leq i \rangle$ for each $1 \leq i \leq \frac{d}{p}$. Then R is a Sylow p-subgroup of H, $\sigma \in N_G(H)$ and $\langle \sigma \rangle \cdot R$ is a Sylow p-subgroup of $N_G(H)$. Therefore, we may assume that $g = \sigma M$ for some matrix M in R.

For each $0 \leq k \leq \frac{d}{p}$ let

$$V_k = \{ v_i x^{q^j} \,|\, 1 \leq i \leq k \,, 0 \leq j \leq p-1 \} \,.$$

Then $\{0\} = V_0 < V_1 < \ldots < V_{\frac{d}{r}} = V$ and for any k, V_k / V_{k-1} as a vector space over $\mathbf{F}_q$ is generated by the set $\{ v_k x^{q^j} + V_{k-1} \,|\, 0 \leq j \leq p-1 \}$. Note that M acts trivially on V_k / V_{k-1} and σ maps $v_k x^{q^j} + V_{k-1}$ to $v_k x^{q^{j+1}} + V_{k-1}$, therefore $\{0\} = V_0 < V_1 < \ldots < V_{\frac{d}{p}} = V$ is a composition series of the $\mathbf{F}_q\langle g \rangle$-module V with each of its quotient isomorphic to the regular $\mathbf{F}_q\langle g \rangle$-module. This means that V is isomorphic to a direct sum of $\frac{d}{p}$ copies of the regular $\mathbf{F}_q\langle g \rangle$-module. ∎

Theorem 4.5.2 *Let $G = GL_d(q)$, $GL_{\frac{d}{p}}(q^p) \simeq H < G$ and $g \in N_G(H) \backslash H$ an element of order p.*

(a) *If $d \neq p$ and $(d,p) \neq (4,2)$ then* $\mu(G, N_G(H), g) \leq \dfrac{1}{q^{d(r-1)}}$;

(b) *If $(d,p) = (4,2)$ and $q = 2$ then* $\mu(G, N_G(H), g) < \dfrac{1}{7}$;

(c) *If $(d,p) = (4,2)$ and $q \geq 4$ then* $\mu(G, N_G(H), g) < \dfrac{3}{q^4}$;

(d) *If $d = p$ then* $\mu(G, N_G(H), g) < \dfrac{2}{q^{(p-1)^2}}$.

Proof: From Theorem 3.1.3,

$$|C_G(g)| = q^{p\left(\frac{d}{p}\right)^2} \cdot \prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^k}\right) = q^{\frac{d^2}{p}} \cdot \prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^k}\right) .$$

Eventually we will use Lemma 4.1.2, but in order to do that, we need an upper bound for $|\mathcal{C}(G, N_G(H), g)|$. If $h \in H$ is conjugate to g in G then h is a homogeneous element of order p in $H \simeq \mathrm{GL}_{\frac{d}{p}}(q^p)$. Now, there is only one conjugacy class of such elements in $\mathrm{GL}_{\frac{d}{p}}(q^p)$ and by Theorem 3.1.3, the cardinality of it is

$$\frac{|\mathrm{GL}_{\frac{d}{p}}(q^p)|}{(q^p)^{p\left(\frac{d}{p^2}\right)^2} \cdot \prod_{k=1}^{\frac{d}{p^2}} \left(1 - \frac{1}{q^{pk}}\right)} = q^{\frac{d^2}{p} - \frac{d^2}{p^2}} \cdot \frac{\prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^{pk}}\right)}{\prod_{k=1}^{\frac{d}{p^2}} \left(1 - \frac{1}{q^{pk}}\right)}$$

and we have

$$\mathcal{C}(G, H, g) \leq q^{\frac{d^2}{p} - \frac{d^2}{p^2}} .$$

Furthermore, from Lemma 4.3.8, the number of elements of order p in $N_G(H) \setminus H$ is at most

$$(p-1) \cdot \frac{|\mathrm{GL}_{\frac{d}{p}}(q^p)|}{|\mathrm{GL}_{\frac{d}{p}}(q)|} = (p-1) q^{\frac{d^2}{p} - \frac{d^2}{p^2}} \cdot \frac{\prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^{pk}}\right)}{\prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^{k}}\right)} < (p-1) q^{\frac{d^2}{p} - \frac{d^2}{p^2}} .$$

The above gives us

$$|\mathcal{C}(G, N_G(H), g)| < p \cdot q^{\frac{d^2}{p} - \frac{d^2}{p^2}} \leq q^{\frac{d^2}{p} - \frac{d^2}{p^2} + 1} .$$

Now, by Lemma 4.1.2,

$$\begin{aligned} \mu(G, N_G(H), g) &= \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H), g)|}{|G|} \\ &< \frac{q^{\frac{d^2}{p}} \cdot \prod_{k=1}^{\frac{d}{p}} \left(1 - \frac{1}{q^k}\right) \cdot q^{\frac{d^2}{p} - \frac{d^2}{p^2} + 1}}{q^{d^2} \prod_{k=1}^{d} \left(1 - \frac{1}{q^k}\right)} \\ &= q^{-d^2(1 + \frac{1}{p^2} - \frac{2}{p}) + 1} \cdot \frac{1}{\prod_{k=\frac{d}{p}+1}^{d} \left(1 - \frac{1}{q^k}\right)} \\ &< 2 \cdot q^{-\left(\frac{(p-1)d}{p}\right)^2 + 1} \end{aligned}$$

since

$$\prod_{k=\frac{d}{p}+1}^{d} \left(1 - \frac{1}{q^k}\right) \geq \prod_{k=2}^{\infty} \left(1 - \frac{1}{q^k}\right) > 1 - \sum_{k=2}^{\infty} \frac{1}{q^k} = 1 - \frac{1}{q^2 - q} \geq \frac{1}{2} .$$

Statement (a) now follows if we can prove that

$$-\left(\frac{(p-1)d}{p}\right)^2 + 2 \leq -d(p-1) ,$$

that is,

$$(p-1)d+2 \leq \big(\frac{(p-1)d}{p}\big)^2 ,$$
$$1+\frac{2}{(p-1)d} \leq \frac{(p-1)d}{p^2} .$$

Taking $n = \frac{d}{p}$ this is equivalent to

$$1+\frac{2}{np(p-1)} \leq \frac{n(p-1)}{p}$$

and this is true whenever $n \geq 3$ or $n = 2$ and $p \geq 3$.

Suppose $(d,p) = (4,2)$. Then as above,

$$|C_G(g)| = q^{p\left(\frac{d}{p}\right)^2} \cdot \prod_{k=1}^{\frac{d}{p}} \left(1-\frac{1}{q^k}\right) = q^8 \cdot \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right) ,$$

$$\mathcal{C}(G,H,g) \leq q^{\frac{d^2}{p}-\frac{d^2}{p^2}} \cdot \frac{\prod_{k=1}^{\frac{d}{p}} \left(1-\frac{1}{q^{pk}}\right)}{\prod_{k=1}^{\frac{d}{p^2}} \left(1-\frac{1}{q^{pk}}\right)} = q^4 \cdot \left(1-\frac{1}{q^4}\right) = q^4-1 ,$$

the number of involutions in $N_G(H) \setminus H$ is

$$\frac{|\mathrm{GL}_2(q^2)|}{|\mathrm{GL}_2(q)|} = q^4+q^3+q^2+q ,$$

and

$$|G| = q^{16} \prod_{k=1}^{4} \left(1-\frac{1}{q^k}\right) .$$

This leads to

$$\mu(G, N_G(H), g) \leq \frac{(q^4-1)+(q^4+q^3+q^2+q)}{q(q^3-1)(q^4-1)} .$$

If $q = 2$ then the right hand side here is $\frac{29}{210} < \frac{1}{7}$ and if $q \geq 4$ then

$$\frac{2q^4+q^3+q^2+q-1}{q^8-q^5-q^4+q} < \frac{2q^4+2q^3}{q^8-2q^5} = \frac{1}{q^4} \cdot \frac{2+\frac{2}{q}}{1-\frac{2}{q^3}} < \frac{3}{q^4} .$$

Finally, assume that $d = p$. Then as above,

$$|C_G(g)| = q^{p\left(\frac{d}{p}\right)^2} \cdot \prod_{k=1}^{\frac{d}{p}} \left(1-\frac{1}{q^k}\right) = q^p\left(1-\frac{1}{q}\right) ,$$

there are no elements of order p in $H \simeq Z_{q-1}$, the number of elements of order p in $N_G(H) \setminus H$ is

$$\frac{|\mathrm{GL}_1(q^p)|}{|\mathrm{GL}_1(q)|} = \frac{q^p - 1}{q - 1} ,$$

hence

$$\begin{aligned} \mu(G, N_G(H), g) &\leq \frac{q^p\left(1-\frac{1}{q}\right) \cdot \frac{q^p-1}{q-1}}{q^{p^2} \prod_{k=1}^{p} \left(1-\frac{1}{q^k}\right)} \\ &= \frac{1}{q^{p^2-2p+1} \prod_{k=1}^{p-1} \left(1-\frac{1}{q^k}\right)} \\ &= \frac{1}{q^{(p-1)^2} \prod_{k=1}^{p-1} \left(1-\frac{1}{q^k}\right)} \\ &\leq \frac{2}{q^{(p-1)^2}} . \end{aligned}$$

The proof of this Theorem is now complete. ■

Theorem 4.5.3 *Let $G = SP_d(q)$, $q = p^f$, p and odd prime divisor of d, $Sp_{\frac{d}{p}}(q^p) \simeq H < G$ and $g \in N_G(H) \setminus H$ an element of order p. Then*

$$\mu(G, N_G(H), g) \leq \frac{1}{q^{\frac{1}{2}d(p-1)}} .$$

Proof: We will follow exactly the same line of reasoning as in the proof of the previous theorem. By Theorem 3.2.16,

$$|C_G(g)| = q^{\frac{d^2}{2p}+\frac{d}{2p}} \prod_{k=1}^{\frac{d}{2p}} \left(1 - \frac{1}{q^{2k}}\right) .$$

Since p is odd, by Theorem 3.2.17, h may have only one conjugacy class that is conjugate to g in G, and if $h \in H$ is conjugate to g then d has to be divisible by p^2 and

$$C_H(h) = q^{\frac{1}{2}\frac{d^2}{p^2}+\frac{d}{2p}} \prod_{k=1}^{\frac{d}{2p^2}} \left(1 - \frac{1}{q^{2k}}\right) ,$$

$$\begin{aligned} |h^H| &= \frac{q^{\frac{d^2}{2p}+\frac{d}{2}} \prod_{k=1}^{\frac{d}{2p}} \left(1-\frac{1}{q^{2k}}\right)}{q^{\frac{1}{2}\frac{d^2}{p^2}+\frac{d}{2p}} \prod_{k=1}^{\frac{d}{2p^2}} \left(1-\frac{1}{q^{2k}}\right)} \\ &< q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)} , \end{aligned}$$

and by Lemma 4.3.9, the number of elements of order p in $N_G(H) \setminus H$ is at most

$$(p-1)\frac{|\mathrm{Sp}_{\frac{d}{p}}(q^p)|}{|\mathrm{Sp}_{\frac{d}{p}}(q)|} = (p-1)\frac{q^{\frac{d^2}{2p}+\frac{d}{2}}\prod_{k=1}^{\frac{d}{2p}}\left(1-\frac{1}{q^{2pk}}\right)}{q^{\frac{d^2}{2p}+\frac{d}{2p}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{1}{q^{2pk}}\right)} < (p-1)q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)} ,$$

hence

$$|\mathcal{C}(G, N_G(H), g)| < p \cdot q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)} \leq q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+1} .$$

Then by Lemma 4.1.2,

$$\begin{aligned}
\mu(G, N_G(H), g) &= \frac{|C_G(g)| \cdot |\mathcal{C}(G, N_G(H))|}{|G|} \\
&< \frac{q^{\frac{d^2}{2p}+\frac{d}{2p}} \cdot q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+1}}{q^{\frac{d^2}{2}+\frac{d}{2}}\prod_{k=1}^{\frac{d}{2}}\left(1-\frac{1}{q^{2k}}\right)} \\
&< \frac{q^{\frac{d^2}{2p}+\frac{d}{2p}} \cdot q^{\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+1}}{q^{\frac{d^2}{2}+\frac{d}{2}-\frac{1}{2}}} \\
&= q^{-\frac{1}{2}\cdot\frac{p-1}{p}(d^2+d)+\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+\frac{3}{2}} ,
\end{aligned}$$

and the statement of this Theorem is true whenever

$$\begin{aligned}
-\frac{1}{2}\cdot\frac{p-1}{p}(d^2+d)+\frac{1}{2}(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+\frac{3}{2} &\leq -\frac{1}{2}d(p-1) , \\
d(p-1)+(p-1)\left(\frac{d^2}{p^2}+\frac{d}{p}\right)+3 &\leq \frac{p-1}{p}(d^2+d) , \\
d+\frac{d^2}{p^2}+\frac{d}{p}+\frac{3}{p-1} &\leq \frac{d^2+d}{p} .
\end{aligned}$$

Since $d = np$ for some positive even integer n, this is equivalent to

$$\begin{aligned}
np+n^2+n+\frac{3}{p-1} &\leq n^2p+n , \\
np+n^2+\frac{3}{p-1} &\leq n^2p , \\
\frac{1}{n}+\frac{1}{p}+\frac{3}{n^2p(p-1)} &\leq 1 .
\end{aligned}$$

Since $p \geq 3$ and $n \geq 2$, we

$$\frac{1}{n}+\frac{1}{p}+\frac{3}{n^2p(p-1)} \leq \frac{1}{2}+\frac{1}{3}+\frac{3}{24} = \frac{23}{24} < 1$$

and this completes the proof. ∎

4.6 Upper Bounds for the Fixed Point Ratios of Arbitrary Elements

Theorem 4.6.1 *Let* $G = GL_d(q)$, $d \geq 3$, $(d,q) \neq (3,4)$, $GL_{\frac{d}{r}}(q^r) \simeq H < G$ *with* r *a prime divisor of* d *and let* $g \in G \setminus Z(G)$.

(a) Suppose d *is a prime number. Then*

$$\mu(G, N_G(H), g) \leq \begin{cases} \frac{7(d-1)}{2^{(d-1)^2}} & \text{if } q = 2 \ ; \\ \frac{3(d-1)}{3^{(d-1)^2}} & \text{if } q = 3 \ ; \\ \frac{2(d-1)}{q^{(d-1)^2}} & \text{if } q \geq 4 \ . \end{cases}$$

(b) Suppose $d = 4$ *and* $r = 2$. *Then*

$$\mu(G, N_H(H), g) < \begin{cases} \frac{1}{5} & \text{if } q = 2 \ ; \\ \frac{1}{19} & \text{if } q = 3 \ ; \\ \frac{3}{q^4} & \text{if } q \geq 4 \ . \end{cases}$$

(c) Suppose $d = 2r \geq 6$. *Then*

$$\mu(G, N_G(H), g) < \frac{3}{q^{d(r-1)}} \ .$$

(d) Suppose $d > 2r$. *Then*

$$\mu(G, N_G(H), g) \leq \frac{1}{q^{d(r-1)}} \ .$$

Proof: Since for any $g \in G$ and positive integer k,

$$\mu(G, N_G(H), g) \leq \mu(G, N_G(H), g^k) \ ,$$

it is enough to prove this theorem for elements that have prime order modulo the center of G. Furthermore, if $g \in G$ ha order p modulo the center, then there exists an α in $\mathbf{F}_q$ such that $g^p = \alpha I$ and $(\alpha^{-1}g)^p = I$, and clearly $\mu(G, N_G(H), g) = \mu(G, N_G(H), \alpha g)$. This implies that it is enough to prove this theorem for elements of order p and for those p'-elements that have a prime order modulo $Z(G)$. These are the elements we studied in the previous four sections. Now, (a) follows from Lemma 4.2.10, Lemma 4.3.17 and Theorem 4.5.2/(d); part (b) follows from Theorem 4.2.9, Lemma 4.3.13, Theorem 4.4.1/(a) and Theorem 4.5.2/(b), (c); part (c) follows from Theorem 4.2.9, Lemma 4.3.12, Theorem 4.4.1/(a) and Theorem 4.5.2/(a);

and statement (d) follows from Theorem 4.2.9, Lemma 4.3.12, Lemma 4.3.13, Theorem 4.4.1/(b) and Theorem 4.5.2/(a). ∎

Theorem 4.6.2 *Let* $G = Sp_d(q)$, q *odd,* $\frac{d}{r}$ *even,* $(d,q) \neq (4,3)$, $Sp_{\frac{d}{r}}(q^r) \simeq H < G$ *with* r *a prime divisor of* d *and let* $g \in G \setminus Z(G)$. *Then*

$$\mu(G, N_G(H), g) \leq \begin{cases} \frac{q}{q^2-1} & \textit{if } d = 4 \textit{ and } r = 2 \ ; \\ \frac{3}{q^{r(r-1)}} & \textit{if } d > 4 \textit{ and } r = \frac{d}{2} \ ; \\ \frac{1}{q^{\frac{1}{2}d(r-1)}} & \textit{if } r \leq \frac{d}{2} \ . \end{cases}$$

Proof: For the same reason as in the previous theorem, it is sufficient to prove these inequalities for those elements discussed in Sections 4.2-4.5. The $(d,r) = (4,2)$ case follows from Theorem 4.2.20/(b), Lemma 4.3.15/(b) and Theorem 4.4.4/(a). The $d = 2r > 4$ case follows from Theorem 4.2.20/(b), Lemma 4.3.15/(a), Theorem 4.4.4/(a) and Theorem 4.5.3. Finally, the $r \leq \frac{d}{2}$ follows from Theorem 4.2.20/(a), Lemma 4.3.14, Lemma 4.3.15/(a), Theorem 4.4.4/(b) and Theorem 4.5.3. ∎

Theorem 4.6.3 *Let* $G = Sp_d(q)$, q *and* $\frac{d}{2}$ *odd, either* $d > 2$ *or* $q \notin \{2,3,5,7,9\}$, $GU_{\frac{d}{2}}(q^2) \simeq H < G$ *and let* $g \in G \setminus Z(G)$. *Then*

$$\mu(G, N_G(H), g) \leq \begin{cases} \frac{1}{q} & \textit{if } d = 2 \textit{ and } q \equiv 1 \ (\textit{mod } 4) \ ; \\ \frac{q+3}{q(q-1)} & \textit{if } d = 2 \textit{ and } q \equiv 3 \ (\textit{mod } 4) \ ; \\ \frac{1}{q^{d-2}} & \textit{if } d \geq 6 \ . \end{cases}$$

Proof: The $d = 2$ case follows from Lemma 4.2.10 and Lemma 4.3.16 and the $d \geq 6$ case follows from Theorem 4.2.21, Lemma 4.3.16/(c) and Theorem 4.4.5. ∎

CHAPTER 5
LOWER BOUNDS FOR THE CARDINALITY OF A(G)

Notation: Let G be a finite projective special linear or a finite projective symplectic group. For a prime divisor r of d, let $\mathcal{M}_r$ denote set of the extension field type maximal subgroups of G that correspond to the prime r, let M_r be a representative element of $\mathcal{M}_r$ and let

$$\mu(\mathcal{M}_r) = \max_{1 \neq g \in G} \mu(G, M_r, g) .$$

Notice that $\mu(\mathcal{M}_r)$ does not depend on the choice of M_r.

We call a set $\mathcal{S} \subset G \setminus \{1\}$ **weakly anti-generating** if for every Singer element x of G there is an element s in $\mathcal{S}$ such that $\langle x, s \rangle \neq G$. Furthermore, let $A_w(G)$ denote the minimal possible cardinality of a weakly anti-generating set of G.

Lemma 5.1 *Let $G = PSL_d(q)$ with $d \geq 3$ and $(d,q) \neq (3,4)$ or $G = PSp_d(q)$ with q odd and $(d,q) \notin \{(2,3),(2,5),(2,7),(2,9),(4,3)\}$. Then*

$$A_w(G) \cdot \Big(\sum_{r \in \pi(d)} \mu(\mathcal{M}_r) \Big) \geq 1 .$$

Proof: With the above conditions for G, the set of maximal overgroups of a Singer element x consists of one representative group from each set $\mathcal{M}_r$. This means that for any $1 \neq g \in G$, the probability of $\langle g, s \rangle \neq G$ is at most $\big(\sum_{r \in \pi(d)} \mu(\mathcal{M}_r) \big)$. Hence for any weakly anti-generating set $\mathcal{S}$ we must have

$$|\mathcal{S}| \cdot \Big(\sum_{r \in \pi(d)} \mu(\mathcal{M}_r) \Big) \geq 1$$

and this implies the statement. ∎

Theorem 5.2 *Let $G = PSL_d(q)$ with $d \geq 3$ and $(d,q) \neq (3,4)$.*

(a) If d is a prime number and $q = 2$ then $A_w(G) \geq \frac{2^{(d-1)^2}}{7(d-1)}$;

(b) If d is a prime number and $q = 3$ then $A_w(G) \geq \frac{3^{(d-1)^2}}{3(d-1)}$;

(c) If d is a prime number and $q \geq 4$ then $A_w(G) \geq \frac{q^{(d-1)^2}}{2(d-1)}$;

(d) If $d = 4$ and $q = 2$ then $A_w(G) \geq 6$;

(e) If $d = 4$ and $q = 3$ then $A_w(G) \geq 20$;

(f) If $d = 4$ and $q \geq 4$ then $A_w(G) \geq \frac{q^4}{3}$;

(g) If $d = 6$ then $A_w(G) \geq q^d - 2$;

(h) If $d > 6$ and d is not a prime then $A_w(G) \geq q^d$.

Actually, if r is the smallest prime divisor of d and $r \geq 3$ then $A_w(G) \geq q^{(r-1)d} - q^{(r-3)d} + 1$.

Proof: The entire proof is based on using Lemma 5.1 and the results of Theorem 4.6.1. If d is a prime then $A_w(G) \cdot \mu(\mathcal{M}d) \geq 1$ and the statement follows immediately from Theorem 4.6.1/(a). If $d = 4$ then similarly, $A_w(G) \cdot \mu(\mathcal{M}_2) \geq 1$ and statements (d), (e) and (f) follow from Theorem 4.6.1/(b).

Suppose $d = 6$. Then

$$A_w(G) \cdot \Big(\mu(\mathcal{M}_2) + \mu(\mathcal{M}_3)\Big) \geq 1 \,,$$

$$\mu(\mathcal{M}_2) + \mu(\mathcal{M}_3) \leq \frac{1}{q^{6(2-1)}} + \frac{3}{q^{6(3-1)}} = \frac{1}{q^6} + \frac{3}{q^{12}} = \frac{q^6 + 3}{q^{12}} \,,$$

$$A_w(G) \geq \frac{q^{12}}{q^6 + 3} = \frac{q^6(q^6+3) - 3q^6}{q^6 + 3} = q^6 - \frac{3q^6}{q^6+3} > q^6 - 3 \,.$$

Suppose $d = 2r$ with a prime number r that is at least 5. Then

$$A_w(G) \cdot \Big(\mu(\mathcal{M}_2) + \mu(\mathcal{M}_r)\Big) \,,$$

$$\mu(\mathcal{M}_2) + \mu(\mathcal{M}_r) \leq \frac{1}{q^{d(2-1)}} + \frac{3}{q^{d(r-1)}} = \frac{q^{2r(r-2)} + 3}{q^{2r(r-1)}} \,,$$

$$A_w(G) \geq \frac{q^{2r(r-1)}}{q^{2r(r-2)} + 3} = \frac{q^{2r}(q^{2r(r-2)} + 3) - 3q^{2r}}{q^{2r(r-2)} + 3} = q^{2r} - \frac{3q^{2r}}{q^{2r(r-2)+3}} > q^d - 1 \,.$$

Finally, suppose that d is neither a prime number nor twice a prime. Then

$$\sum_{r\in\pi(d)} \mu(\mathcal{M}_r) \le \sum_{r\in\pi(d)} \frac{1}{q^{d(r-1)}} < \sum_{k=1}^{\infty} \frac{1}{q^{dk}} = \frac{1}{q^d-1} ,$$

$$A_w(G) > q^d - 1 .$$

If r is the smallest prime divisor of d and $r \ge 3$ then

$$\sum_{r\in\pi(d)} \mu(\mathcal{M}_r) \le \sum_{k=0}^{\infty} \frac{1}{q^{d(r-1+2k)}} = \frac{1}{q^{d(r-1)}} \cdot \frac{q^{2d}}{q^{2d}-1}$$

$$A_w(G) > \frac{q^{d(r-1)} \cdot (q^{2d}-1)}{q^{2d}} = q^{q(r-1)} - q^{d(r-3)} . \quad \blacksquare$$

Theorem 5.3 *Let* $G = PSp_d(q)$ *with* q *odd and* $(d,q) \neq (4,3)$, $(2,3)$, $(2,5)$, $(2,7)$ *or* $(2,9)$.

(a) If $d = 2$ *and* $q \equiv 1 \pmod 4$ *then* $A_w(G) \ge q$;

(b) If $d = 2$ *and* $q \equiv 3 \pmod 4$ *then* $A_w(G) \ge \frac{q(q-1)}{q+3}$;

(c) If $d = 4$ *then* $A_w(G) \ge q$;

(d) If $d = 6$ *then* $A_w(G) \ge q^4 - 3q^2$;

(e) If $d = 2r$ *with a prime number* $r \ge 5$ *then* $A_w(G) \ge q^{d-2}$;

(f) If $d = 2r$ *with* r *an odd composite number then* $A_w(G) \ge q^{d-2} - q^{d-4}$;

(g) If $d \equiv 0 \pmod 4$ *and* $d \ge 8$ *then* $A_w(G) \ge q^{\frac{1}{2}d}$.

Proof: The proof is based on Lemma 5.1 and the results of Theorem 4.6.2 and Theorem 4.6.3. Parts (a), (b) and (c) are straightforward form these theorems.

Suppose $d = 6$. Then

$$A_w(G) \cdot \Big(\mu(\mathcal{M}_2) + \mu(\mathcal{M}_3)\Big) \ge 1 ,$$

$$\mu(\mathcal{M}_2) + \mu(\mathcal{M}_3) \le \frac{1}{q^{6-2}} + \frac{3}{q^{3(3-1)}} = \frac{1}{q^4} + \frac{3}{q^6} = \frac{q^2+3}{q^6} ,$$

$$A_w(G) \ge \frac{q^6}{q^2+3} = \frac{q^4(q^2+3) - 3q^4}{q^2+3} = q^4 - \frac{3q^4}{q^2+3} > q^4 - 3q^2 .$$

Suppose $d = 2r$, r a prime number and $r \geq 5$. Then

$$A_w(G) \cdot \Big(\mu(\mathcal{M}_2) + \mu(\mathcal{M}_r)\Big) \geq 1 \,,$$

$$\mu(\mathcal{M}_2) + \mu(\mathcal{M}_r) \leq \frac{1}{q^{2r-2}} + \frac{3}{q^{r(r-1)}} = \frac{q^{(r-2)(r-1)} + 3}{q^{r(r-1)}} \,,$$

$$A_w(G) \geq \frac{q^{r(r-1)}}{q^{(r-2)(r-1)} + 3} = \frac{q^{2(r-1)}(q^{(r-2)(r-1)} + 3) - 3q^{2(r-1)}}{q^{(r-2)(r-1)} + 3} =$$

$$= q^{2(r-1)} - \frac{3q^{2(r-1)}}{q^{(r-2)(r-1)} + 3} > q^{2(r-1)} - 1 \,.$$

Suppose $d = 2r$ with r an odd number, which is a product of at least two primes. Then

$$\sum_{r \in \pi(d)} \mu(\mathcal{M}_r) \leq \frac{1}{q^{d-2}} + \sum_{s \in \pi\left(\frac{d}{2}\right)} \frac{1}{q^{\frac{1}{2}d(s-1)}} < \frac{1}{q^{d-2}} + \sum_{k=1}^{\infty} \frac{1}{q^{dk}} =$$

$$= \frac{1}{q^{d-2}} + \frac{1}{q^d - 1} = \frac{q^d + q^{d-2} - 1}{q^{2d-2} - q^{d-2}} \,,$$

$$A_w(G) > \frac{q^{2d-2} - q^{d-2}}{q^d + q^{d-2} - 1} > \frac{q^{2d-2} - q^{d-2}}{q^d + q^{d-2}} = \frac{q^d - 1}{q^2 + 1} =$$

$$= \frac{q^{d-2}(q^2 + 1) - q^{d-2}}{q^2 + 1} > q^{d-2} - q^{d-4} \,.$$

Finally, suppose $d \equiv 0 \pmod 4$ and d is at least 8. Then

$$\sum_{r \in \pi(d)} \mu(\mathcal{M}_r) \leq \sum_{r \in \pi(d)} \frac{1}{q^{\frac{1}{2}d(r-1)}} < \sum_{k=1}^{\infty} \frac{1}{q^{\frac{1}{2}dk}} = \frac{1}{q^{\frac{1}{2}d} - 1} \,,$$

$$A_w(G) > q^{\frac{d}{2}} - 1 \,. \quad \blacksquare$$

Theorem 5.4 *Let $G \simeq PSL_2(q)$ with $q \geq 4$.*

(*a*) *If q is even then $A(G) = A_w(G) = q - 1$;*

(*b*) *If $q \equiv 1$ (mod 4) and $q \geq 13$ then $A(G) = A_w(G) = q$;*

(*c*) *If $q \equiv 3$ (mod 4) and $q \geq 11$ then $A(G) \geq q - 3$;*

(*d*) *If $q = 5$ or $q = 9$ then $A(G) = 3$;*

(*e*) *If $q = 7$ then $A(G) = 5$.*

Proof: (*a*) Suppose $q = 2^f$ with $f \geq 2$. By Theorem 2.3.6 the only maximal subgroups of $\mathrm{PSL}_2(q)$ containing a Singer cycle are isomorphic to the dihedral group $D_{2(q+1)}$ of cardinality $2(q+1)$. Let S be a fixed Singer cycle of G and let N be the normalizer of S in G. Now if $1 \neq g \in S$ then by the formula given in Lemma 4.1.2,

$$\mu(G,N,g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G,N,g)|}{|G|} = \frac{|S| \cdot 1}{|G|} = \frac{q+1}{(q-1)q(q+1)} = \frac{1}{(q-1)q},$$

and if $g \in N \setminus S$ then

$$\mu(G,N,g) = \frac{|C_G(g)| \cdot |\mathcal{C}(G,N,g)|}{|G|} = \frac{q \cdot (q+1)}{(q-1)q(q+1)} = \frac{1}{q-1}.$$

Therefore,

$$\mu(\mathcal{M}_2) = \frac{1}{q-1}$$

and as in Lemma 5.1,

$$A_w(G) \cdot \frac{1}{q-1} \geq 1,$$
$$A_w(G) \geq q-1.$$

On the other hand, we will show that the non-trivial elements of a Sylow 2-subgroup P of G form an anti-generating set. Notice that every element of G is either an involution, or is contained in a cyclic subgroup of order $q+1$ or $q-1$. Obviously, if $g \in G$ is an involution then $\langle g, x\rangle \neq G$ for any $x \in P^\# = P \setminus \{1\}$. Suppose $g \in G$ and g is contained in a cyclic subgroup H of order $q+1$. Then $P \cap N_G(H)$ must be non-trivial, since $N_G(H)$ contains $q+1$ involutions, the same number as the number of Sylow 2-subgroups in G, and no Sylow 2-subgroup can have more then one involution in common with $N_G(H)$ (as any two involutions in P generate a subgroup of order 4 and 4 does not divide the order of $N_G(H)$). So there is a non-trivial element x in $P \cap N_G(H)$, for which then $\langle g, x\rangle \neq G$. Now suppose $g \in G$ and g is contained in a cyclic subgroup H of cardinality $q-1$. If H normalizes P then obviously $\langle g, x\rangle \neq G$ for any x in $P^\#$, so let us assume that H does not normalize P. Now, $N_G(H) \setminus H$ is a set of $q-1$ involutions, none of which belong to a Sylow

2-subgroup that normalizes P. Furthermore, no Sylow 2-subgroup can contain more then one of these involutions. And since the number of Sylow 2-subgroups of G not normalizing H is exactly $q-1$, it follows that $N_G(H)$ has a non-trivial intersection with any Sylow 2-subgroup of G that does not normalize H. In particular, there is a non-trivial element x in $P \cap N_G(H)$, for which then $\langle g, x\rangle \neq G$. This shows that $P^{\#}$ is an anti-generating set in G.

(*b*) Suppose $q = p^f \equiv 1 \pmod 4$ and $q \geq 13$. By Theorem 5.3/(*a*), $A(G) \geq q$. In order to prove that $A(G) = q$, we will give an example of an anti-generating set in G of cardinality q. Let P be a Sylow p-subgroup of G and let $N = N_G(P)$. Then $N \simeq Z_{\frac{q-1}{2}} \ltimes P$ and N contains q cyclic subgroups of order $\frac{q-1}{2}$, with any two of them intersecting trivially. In particular, N contains q involutions. Let X denote the set of involutions of N; we will show that X is an anti-generating set in G. In order to do that, first notice that every element of G belongs either to a Singer cycle of G (that is, a cyclic subgroup of order $\frac{q+1}{2}$) or to the normalizer of a Sylow p-subgroup. Now let g be any element of G. If $g \in N_G(Q)$ for a Sylow p-subgroup Q of G then since $N_G(P)$ and $N_G(Q)$ have a cyclic subgroup of order $\frac{q-1}{2}$ in common, $\langle g, x\rangle \leq N_G(Q)$ for a suitable $x \in X$. If $g \in S$ for a Singer cycle S in G then $\langle g, x\rangle \leq N_G(S)$ for a suitable $x \in X$. This is true because $N_G(S) \setminus S$ consists of $\frac{q+1}{2}$ involutions, every one of them is normalizing two Sylow p-subgroups of G, no two of then can normalize the same Sylow p-subgroup, and the number of Sylow p-subgroups of G is exactly $q+1$. This implies that one of the involutions of $N_G(S)$ normalizes P and thus belongs to X. The above arguments show that X is indeed an anti-generating set in G.

Statement (*c*) follows immediately from Theorem 5.3/(*b*) since $\frac{q(q-1)}{q+3} > q-4$ for any positive integer q. Also, for $q = 5$, (*d*) follows from (*a*) as $\mathrm{PSL}_2(5) \simeq \mathrm{PSL}_2(4)$.

To prove (*d*) for $q = 9$, let G be the alternating group A_6 and we will show that $A(G) = 3$. First we give an example for an anti-generating set in G with cardinality 3. Let $X = \{(1\,2)(3\,4),\ (1\,2)(5\,6),\ (3\,4)(5\,6)\}$. If $g \in G$ and g stabilizes a point $\alpha \in \{1,2,3,4,5,6\}$ then obviously $\langle g, x\rangle \leq G_\alpha$ for some $x \in X$. If g does not stabilize any point then g is either a product of two 3-cycles or the product of a 2-cycle and a 4-cycle. Suppose $g = (\alpha\beta\gamma)(\delta\mu\nu)$ with $\{\alpha,\beta,\gamma,\delta,\mu,\nu\} = \{1,2,3,4,5,6\}$. If $\{1,2\} \subset \{\alpha,\beta,\gamma\}$ then $\langle g, x\rangle \leq G_{\{\alpha,\beta,\gamma\}}$ for a suitable $x \in X$ and the same is true if $\{3,4\} \subset \{\alpha,\beta,\gamma\}$ or $\{5,6\} \subset \{\alpha,\beta,\gamma\}$. In any other case, $\langle g, x\rangle$ stabilizes the decomposition $\{1,2,3,4,5,6\} = \{\alpha,\beta,\gamma\} \cup \{\delta,\mu,\nu\}$ for each $x \in X$. Now suppose that $g = (\alpha\beta)(\gamma\delta\mu\nu)$. If $\{\alpha,\beta\} = \{1,2\}$ or $\{3,4\}$ or $\{5,6\}$ then $\langle g, x\rangle \leq G_{\{\alpha,\beta\}}$ for any $x \in X$. Otherwise, for symmetry reasons, we may assume that $(\alpha\beta) = (1\,3)$. Then g stabilizes one of the set decompositions $\{1,3\} \cup \{2,4\} \cup \{5,6\}$, $\{1,2,5\} \cup \{3,4,6\}$ and $\{1,2,6\} \cup \{3,4,5\}$ (corresponding to the cases when $2g^2 = 4$, 5, or 6, respectively). Since all of these three decompositions are also stabilized by $(1\,2)(3\,4)$, it follows that $\langle g, (1\,2)(3\,4)\rangle \neq G$. This shows that X is an anti-generating set in G.

Next, we prove that there is no anti-generating set of cardinality 2 in G. Let $\mathcal{A}$ denote the set of point stabilizers in G and let $\mathcal{B}$ denote the other conjugacy class of the subgroups of G isomorphic to A_5.

Claim 1: A 3-cycle and a 5-cycle generate A_6 unless they have a common fixed point.

Proof: If g is a 3-cycle and h is a 5-cycle with $\langle g, h\rangle$ transitive, then $\langle g, h\rangle$ is also double-transitive. And in general, any double-transitive group that contains a 3-cycle, also contains the whole alternating group.

Claim 2: If g is a 3-cycle and $H \in \mathcal{B}$ then there are 12 5-cycles in H that generate G together with g.

Proof: There are 24 5-cycles in H and every stabilizer subgroup contains exactly four of them. The rest follows from Claim 1.

Claim 3: If g is a product of two disjoint 3-cycles and $H \in \mathcal{A}$ then there are 12 5-cycles in H that generate G together with g.

Proof: This follows from Claim 2, since there is an automorphism of G that moves g into a 3-cycle and moves H into a subgroup in $\mathcal{B}$.

Claim 4: If g is an involution in G then g is contained in two members of $\mathcal{A}$ and in two members of $\mathcal{B}$. Therefore, if $H \in \mathcal{A} \cup \mathcal{B}$ and $g \notin H$ then there are 16 5-cycles in H that generate G together with g.

Proof: The first statement is obvious. Suppose $H \in \mathcal{A}$ with $g \notin H$. Then H has 24 5-cycles, from which 4 is contained in each member of $\mathcal{B}$, so there are 8 of them contained in one of those members of $\mathcal{B}$ containing g. The rest has to generate G together with g.

Claim 5: If g is a 5-cycle, $H \in \mathcal{A} \cup \mathcal{B}$ and $g \notin H$ then there are 20 5-cycles in H that generate G together with g.

Proof: Suppose $H \in \mathcal{A}$. There is one member of $\mathcal{B}$ containing g and it also contains 4 of the 5-cycles of H. Any other 5-cycle of H generates G together with g. A similar argument can be used if $H \in \mathcal{B}$.

Claim 6: If g is an element of order 4 in G then for any 5-cycle $h \in G$, $\langle g, h \rangle = G$.

Proof: Any maximal subgroup of G containing a 5-cycle is isomorphic to A_5, and A_5 does not have elements of order 4.

Claim 7: If g_1 and g_2 are both fixed point free 3-elements in G and $H \in \mathcal{B}$ such that $g_1 \notin H$ and $g_2 \notin H$ then for any 5-cycle $h \in H$, $\langle g_1, h \rangle = \langle g_2, h \rangle = G$.

Proof: Let φ be an automorphism of G that maps g_1 and g_2 into 3-cycles and maps H into a member of $\mathcal{A}$. Then since $g_1, g_2 \notin H$, the fixed point of $H\varphi$ is not a fixed point of g_1 or g_2 and by Claim 1, we have $\langle g_1, h \rangle = \langle g_2, h \rangle = G$.

Claim 8: If g is a 3-cycle and h is the product of two disjoint 3-cycles such that $[g, h] \neq 1$ then $\langle g, h \rangle = G$.

Proof: It is easy to check that $\langle g, h \rangle$ is not only transitive, but it is also a primitive subgroup of G. And since it contains a 3-cycle, we have $\langle g, h \rangle = G$.

Now we are ready to prove that G does not admit an anti-generating set of cardinality 2. Claims 2–6 show that for any element $g \in G$ there is a 5-cycle h such that $\langle g, h \rangle = G$. Therefore, by Claim 6, a set of cardinality 2 containing an element of order 4 cannot be anti-generating. Now suppose $X = \{g_1, g_2\} \subset G$ with g_1 being an involution. If g_2 is a 3-cycle, a product of two disjoint 3-cycles, or a 5-cycle, then by Claims 2, 3 and 5, respectively together with Claim 4 imply that $\langle g_1, h\rangle = \langle g_2, h\rangle = G$ for a suitable 5-cycle h. From now on, we may assume that g_1 and g_2 are elements of order 3 or 5. If one of them has order 5 then by Claims 2, 3 and 5 there is again a 5-cycle h with $\langle g_1, h\rangle = \langle g_2, h\rangle = G$. If g_1 is a 3-cycle and g_2 is a product of two disjoint 3-cycles then Claims 1 and 3 imply that $\{g_1, g_2\}$ cannot be an anti-generating set. Also, if g_1 and g_2 are both 3-cycles having a common fixed point then by Claim 1, and if g_1 and g_2 are both fixed point free 3-elements that do not commute with each other then by Claim 8, there is again a 5-cycle h with $\langle g_1, h\rangle = \langle g_2, h\rangle = G$. Finally, if g_1 and g_2 are both 3-cycles or both fixed point free 3-elements such that $[g_1, g_2] = 1$ then by Claim 8 there exists a 3-element h that generates G together with g_1 and also with g_2.

This completes the proof of statement (d).

Now let $G \simeq \mathrm{PSL}_2(7)$. Let $\mathcal{P}$ be a projective plane of order 7, let P be the set of points and L be the set of lines of $\mathcal{P}$, and let us identify G with the automorphism group of $\mathcal{P}$. Furthermore, for any $p \in P$ and $l \in L$, let G_p and G_l denote the stabilizers of p and l, respectively. We will use the following basic facts:

1. There are three conjugacy classes of maximal subgroups in G, two of these conjugacy classes consists of subgroups isomorphic to S_4 (these are the point stabilizers and line stabilizers), and there is a conjugacy class that consists of eight subgroups, isomorphic to $Z_3 \ltimes Z_7$.

2. There are 6 conjugacy classes of the elements in G, with element orders 1, 2, 3, 4, 7, 7.

3. Every element of order 4 stabilizes a point p and a line l such that $p \in l$. Also, if l is a line and p is a point on l then $|G_p \cap G_l| = 8$ and $G_p \cap G_l$ contains one cyclic subgroup of order 4.
4. Every element of order 3 stabilizes a point p and a line l such that $p \notin l$. Also, if l is a line and p is a point not on l then $|G_p \cap G_l| = 6$ and $G_p \cap G_l$ contains one cyclic subgroup of order 3.
5. If p_1, p_2 and p_3 are the three points of a line l then $G_{p_1,p_2,p_3} \simeq Z_2 \times Z_2$.
6. Every 3-element of G normalizes two cyclic subgroups of order 7.

It is easy to see that there is an anti-generating set of cardinality $A(G)$ in G that contains only elements of order 2 or 3. This is true because in an anti-generating set, any element of order 4 can be replaced by its square and any element of order 7 can be replaced by a 3-element of its unique maximal overgroup. Furthermore, since the unique maximal overgroup of any 7-element is isomorphic to $Z_3 \ltimes Z_7$ and since every 3-element is contained only in two copies of $Z_3 \ltimes Z_7$, it follows that an anti-generating set that does not contain any 7-elements, has to contain at least four 3-elements. But a set of four 3-elements cannot be an anti-generating set. To prove this, suppose g_1, g_2, g_3, and g_4 are 3-elements of G. Since each of them stabilizes only one point, there must be at least five lines in L that contain a point not stabilized by any of the g_i's. And since any 3-element stabilizes only one line, at least one of those five lines are not stabilized by any of the g_i's. That is, there is a line l and a point p such that $p \in l$ and neither p nor l is stabilized by g_1, g_2, g_3 or g_4. Then $G_p \cap G_l$ contains an element h of order 4, and since the only maximal overgroups of h are G_p and G_l, we have $\langle g_i, h\rangle = G$ for $i = 1, 2, 3, 4$.

The above arguments show that an anti-generating set of G has to have a cardinality of at least five. On the other hand, we will construct an anti-generating set of cardinality five. Let l be any line of $\mathcal{P}$ and let p_1, p_2, p_3 and p_4 be the points not on l. Furthermore, for each $1 \leq i \leq 4$, let x_i be a 3-element in $G_{p_i} \cap G_l$ and let x_5 be an involution in the pointwise stabilizer of l. Now, if $h \in G$ and h is not a 7-element then for some $1 \leq i \leq 5$, $\langle h, x_i \rangle$ is contained in a point stabilizer. Furthermore, any subgroup of order 7 is normalized by one of the elements x_1, x_2, x_3 or x_4, since each of these 3-elements normalizes two subgroups of order 7, and no two of them can normalize the same subgroup of order 7. This shows that $X = \{x_1, x_2, x_3, x_4, x_5\}$ is an anti-generating set in G. ■

REFERENCES

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[2] B. N. Cooperstein, *Maximal subgroups of* $G_2(2^n)$, J. Algebra 70, 1981. pp. 23–26

[3] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. 110, 1969. pp. 199–205

[4] R. M. Guralnick, W. M. Kantor, *Probabilistic generation of finite simple groups*, unpublished paper, 1997. University of Southern California, Los Angeles, CA.

[5] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, *Linear groups with orders having certain large prime divisors*, unpublished paper, 1997. University of Southern California, Los Angeles, CA.

[6] W. M. Kantor, *Linear groups containing a Singer cycle*, J. Algebra 62, 1980. pp.232–234

[7] W. M. Kantor, A. Lubotzky, *The probability of generating a finite classical group*, Geom. Ded. 36, 1990. pp. 67–87

[8] M. W. Liebeck, A. Shalev, *The probability of generating a finite simple group*, Geom. Ded. 56, 1995. pp. 103–113

[9] M. W. Liebeck, A. Shalev, *Classical groups, probabilistic methods, and the (2,3)-generation problem*, Ann. of Math. 144, 1996, pp. 77–125

[10] F. Lubeck, G. Malle, *(2,3)-generation of exceptional groups*, J. of London Math. Soc., to appear

[11] G. Malle, J. Saxl, T. Weigel, *Generation of classical groups*, Geom. Ded. 49, 1994, pp. 85–116

[12] E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, Leipzig, 1882. see p. 76

[13] M. Suzuki, *Group Theory, I.* Springer-Verlag, 1982.

[14] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. 3, 1892. pp. 265–284

BIOGRAPHICAL SKETCH

I was born on July 13, 1969 in Budapest, Hungary as the second child of my parents, followed by nine younger brothers and sisters. I attended the doctoral program at the Department of Mathematics, University of Florida since August, 1994. Before that I held a one year position as instructor at the Eötvös University, Budapest, the same place where I received my University Diploma in Mathematics in June, 1993. For the period of the academic year 1991-92, I was a visiting student at the Queen Mary and Westfield College, University of London.

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

John G. Thompson

John G. Thompson, Chairman
Graduate Research Professor
of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Alexandre Turull
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Willis Bodine

Willis R. Bodine
Professor of Music

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

James E. Keesling
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Helmut Voelklein
Professor of Mathematics

This dissertation was submitted to the Graduate Faculty of the Department of Mathematics in the College of Liberal Arts and Sciences and to the Graduate School and was accepted as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

December 1998

Dean, Graduate School